

LSS2200-8P

Managed Layer 2 Gigabit Ethernet PoE++ Switch

(8) 10/100/1000Base-T IEEE 802.3bt + (2) 10G/5G/2.5G/1G SFP+ Multi-Gig Slots

Web User Guide

Part Number 33861
Revision C June 2023

Intellectual Property

© 2022, 2023 Lantronix, Inc. All rights reserved. No part of the contents of this publication may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.

Lantronix is a registered trademark of Lantronix, Inc. in the United States and other countries.

All other trademarks and trade names are the property of their respective holders.

Patented: <https://www.lantronix.com/legal/patents/>; additional patents pending.

Warranty

For details on the Lantronix warranty policy, go to <http://www.lantronix.com/support/warranty>.

Contacts

Lantronix Corporate Headquarters

48 Discovery, Suite 250

Irvine, CA 92618, USA

Toll Free: 800-526-8766

Phone: 949-453-3990

Fax: 949-453-3995

Technical Support

Online: <https://www.lantronix.com/technical-support/>

Sales Offices

For a current list of our domestic and international sales offices, go to www.lantronix.com/about/contact.

Disclaimer

All information contained herein is provided "AS IS." Lantronix undertakes no obligation to update the information in this publication. Lantronix does not make, and specifically disclaims, all warranties of any kind (express, implied or otherwise) regarding title, non-infringement, fitness, quality, accuracy, completeness, usefulness, suitability or performance of the information provided herein. Lantronix shall have no liability whatsoever to any user for any damages, losses and causes of action (whether in contract or in tort or otherwise) in connection with the user's access or usage of any of the information or content contained herein. The information and specifications contained in this document are subject to change without notice.

Revision History

Date	Rev.	Comments
2/27/23	B	FW v 1.6.0.0R6: Add Virtual Cable Test webpage. Add PVLAN Web page and add ConsoleFlow On-premise support. Add option to configure native VLAN ID (PVID) for Trunk mode. Update Digital I/O. Add Telnet warning message. Add support for schedule names with spaces. Note that you must use HTTPS:// in web browsers. Add Port Status 'disabled' and Port Description. Add Cancel button to Reboot webpage. Update File Transfer support and show LLDP Neighbors table. Let Web UI accept schedule date as upcoming date. Add note: If upgrading from v1.5.0.0R16 to v1.6.0.0R6, reload defaults and save or do a factory reset.
6/6/23	C	FW v 1.7.0.0R5: Allow Web UI Admin users to change other users' passwords. Added REST server Deprecation warning for SSLContext. Fixed ConsoleFlow Configuration Editor. Added Web UI dialog for user to change their own password. Added ConsoleFlow support for LLDP Neighbor list. Restructured Port VLAN so Interfaces can be part of PVLAN in the IF config itself. Updated LLDP TxInterval and Holdtime in CLI and Web UI. Updated OpenWRT.

Contents

- 1. Introduction5**
 - Product Description5
 - About This Manual5
 - Related Manuals5
 - Safety Information5
 - Cautions and Warnings5
- 2. Initial Switch Configuration6**
 - Connect and Log In to the Switch Using a Web Browser6
 - Update Password7
- 3. Web User Interface (Web UI) Operation8**
 - Menu System Overview8
 - Webpage Controls and Messages9
 - System10
 - System > System Info10
 - System > IP Settings13
 - Adding a VLAN14
 - Deleting a VLAN14
 - System > IP Status15
 - System > IP Statistics16
 - System > Static Routes17
 - Adding a Static Route17
 - Deleting a Static Route18
 - System > ARP19
 - System > NTP20
 - Adding an NTP Server20
 - Deleting an NTP Server21
 - System > Diagnostics22
 - System > DHCP Relay24
 - System > DHCP Server25
 - Adding a DHCP Server25
 - Modify an Existing DHCP Server32
 - Delete an Existing DHCP Server33
 - System > DHCP Snooping34
 - System > BLE35
 - System > Manage Users36
 - Port Management40
 - Port Management > Port Config40
 - Port Management > Port Status42
 - Port Management > Port Statistics43
 - Port Management > PVLAN Config44
 - Port Management > Port VLAN Config45
 - Port Management > Port Mirroring47
 - Port Management > Port Security48
 - Port Management > Virtual Cable Test50
 - Port Management > Digital IO52
 - Port Management > LLDP54
 - Port Management > Spanning Tree58
 - Port Management > QoS62
 - Port Management > MAC Address Table65
 - Port Management > DDMI66
 - PoE Management67

- PoE Management > PoE Status..... 67
- PoE Management > PoE Config..... 72
- PoE Management > PoE Auto Power Reset..... 74
- PoE Management > PoE Scheduler..... 75
- SNMP 78
 - SNMP > SNMP 78
 - SNMP > SNMPv2 Communities 80
 - SNMP > SNMPv3 Users..... 81
 - SNMP > SNMPv3 Views..... 83
- Notifications 85
 - Notifications > Alarms 85
 - Notifications > Alarm Config 86
 - Notifications > Syslog 88
- Maintenance 90
 - Maintenance > Backup 90
 - Maintenance > Restore 91
 - Maintenance > Save Startup Config..... 92
 - Maintenance > Factory Defaults 93
 - Maintenance > Firmware Update 94
 - Maintenance > Reboot 95
- ConsoleFlow 96
- Lantronix Provisioning Manager (LPM) 100
 - Supported Features 101
 - Discovering Devices 101
- 4. Troubleshooting 102**
- 5. Regulatory Agency Information 102**
- 6. MobileApp 102**

1. Introduction

Product Description

The LSS2200-8P is a managed Layer 2+ Gigabit Ethernet switch offering eight (8) 1GBase-T interfaces with full IEEE 802.3bt 90W support, two (2) 10/5/2.5/1GBase-T multi-gigabit SFP+ slots, two (2) programmable Digital Input/Outputs with 12V power output, and one (1) RJ-45 console port. The switch features Near Field Communications (NFC) support for simplified transfer of pre-configuration onto units prior to powering up and dispatching to install sites through the LSS2200-8P Mobile App (see LSS2200-8P Mobile App User Guide for more information).

The LSS2200-8P switch offers 720W total PoE budget for powering LED lighting, high-powered security and surveillance cameras and other IP devices. Its small footprint and hardened temperature rating make it ideal for powering IP devices distributed throughout a building. The LSS2200-8P also incorporates Bluetooth Low Energy (BLE) for wireless CLI without requiring physical access to troubleshoot, configure or reset the device. Cloud management and APIs for integrating with building management systems make the switch very easy to deploy and manage.

See the LSS2200-8P Install Guide for additional product information.

About This Manual

This manual gives specific information on how to operate and use the management functions of the switch via its Web browser. This manual is intended for use by network administrators who are responsible for operating and maintaining network equipment; it assumes a strong knowledge of Ethernet switch functions, the Internet Protocol (IP), and Hypertext Transfer Protocol (HTTP). Note that this manual may provide links to third party websites for which Lantronix is not responsible.

Related Manuals

- LSS2200-8P Quick Start Guide, 33859
- LSS2200-8P Install Guide, 33860
- LSS2200-8P Web User Guide, 33861
- LSS2200-8P CLI Reference, 33862
- LSS2200-8P REST API User Guide, 33863
- LSS2200-8P MobileApp User Guide, 33870
- Release Notes (revision specific)

Safety Information

Review the following Cautions and Warnings before starting to install the LSS2200-8P. Note that not all Cautions and Warnings apply to every switch environment and application.

Cautions and Warnings

Cautions indicate that there is the possibility of poor equipment performance or potential damage to the equipment. **Warnings** indicate that there is the possibility of injury to person.

Cautions and Warnings appear here and may appear throughout this manual where appropriate. Failure to read and understand the information identified by this symbol could result in poor equipment performance, damage to the equipment, or injury to persons.



Warning: Do not open the chassis - No field serviceable parts.

See the LSS2200-8P Install Guide for additional safety information.

2. Initial Switch Configuration

Connect and Log In to the Switch Using a Web Browser

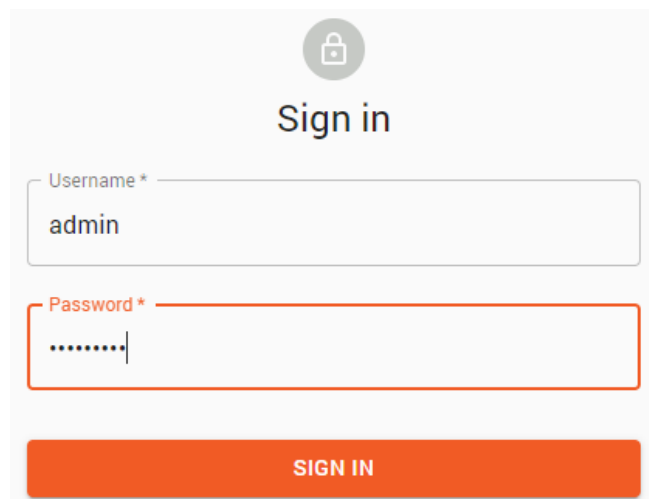
You can perform an initial configuration prior to power up using the NFC Configuration feature on the Mobile App (see LSS2200-8P Mobile App User Guide for more information). Or, after powering up the switch for the first time, you can perform the initial switch configuration using a web browser (you must use https://). For managing other switch features, see the Web User Guide section for details.

To begin the initial configuration stage, you must reconfigure your PC's IP address and subnet mask so as to make sure the PC can communicate with the switch. The switch default IP address is **192.168.60.1**, so the PC needs a different IP address in that subnet, as described in step 2 in the procedure below. The initial Username is **admin** and the initial Password is **ltrx-admin**. You should change the password as soon as possible, because the initial password is known to anyone who reads this manual. You can also change a user name or add new users.

Note: The switch factory default IP address is **192.168.60.1**. The factory default Subnet Mask is **255.255.255.0**.

Initial Switch Configuration Procedure:

1. Power up the PC that you will use for the initial configuration. Please make sure the PC has the Ethernet RJ45 connector to be connected to the switch via standard Ethernet LAN cable.
2. Reconfigure the PC's IP address and Subnet Mask as below, so that it can communicate with the switch. The method to change the PC's IP address varies by operating system.
3. Power up the switch to be initially configured and wait until it has finished its start-up processes. Startup is complete when the Power LED changes from flashing green to solid green.
4. Connect the PC to any port on the switch using a standard Ethernet cable, and check the port LED on the switch to make sure the link status of the PC is OK.
5. Run your Web browser on the PC; enter the factory default IP address to access the switch's Web UI. If your PC is configured correctly, the switch Sign in page displays as shown below.



If you do not see the above login page, perform these steps:

- Refresh the web page.
- Check to ensure use of a secure https:// address.
- Check to see if there is an IP conflict issue.
- Clear browser cookies and temporary internet files.
- Check your PC settings again and repeat step 2.

6. Enter the factory default username (**admin**) and password (**ltrx-admin**) in the Login page and click “Login” to log into the switch. Note that you must use HTTPS:// in web browsers.

When you log in to the Web UI for the first time you are taken to a screen with four entry fields (username, password, new password, confirm password). After you enter the correct default username and password and valid new passwords (minimum length 6 characters) and if the confirm password matches the new password and then click Apply, the password will change and you can log in normally. You can't access anything else on the Web UI until you pass this screen.

Messages: *Incorrect Login and/or Password* displays if the entered Username or Password was entered. **1.** Click OK to clear the message. **2.** Re-enter the correct Username and Password and continue operation.

Update Password

After a successful initial login, you are prompted to change the password as shown and described below. Note that all fields are required.

Username * : Enter the current Username.

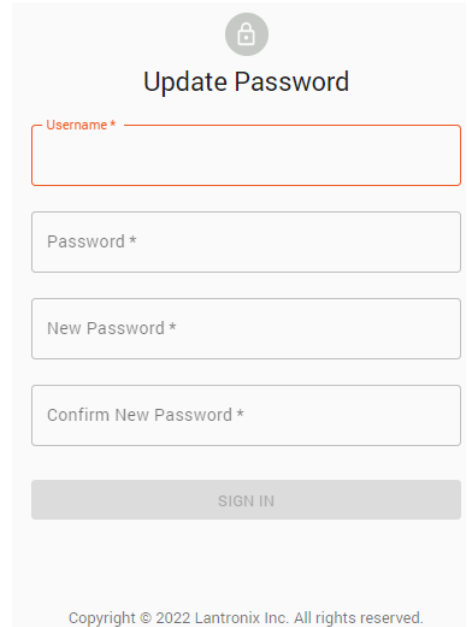
Password * : Enter the current Password.

New Password * : Enter the new Password; this must be at least 6 characters..

Confirm New Password * : Enter the new Password again; it must match the previous entry.

Click SIGN IN when all fields are complete.

After a successful initial login, it is recommended that you save to startup (`copy running-config startup-config`). Otherwise the Update Password page will display again after a Reboot.



3. Web User Interface (Web UI) Operation

Menu System Overview

Main Menu item	Sub-Menus
System	System Info IP Settings IP Status IP Statistics Static Routes ARP NTP Diagnostics DHCP Relay DHCP Server DHCP Snooping BLE Manage Users
Port Management	Port Config Port Status Port Statistics PVLAN Config Port VLAN Config Port Mirroring Port Security Virtual Cable Test Digital IO LLDP Spanning Tree QoS MAC Address Table DDMI
PoE Management	PoE Status PoE Config PoE Auto Power Reset PoE Scheduler
SNMP	SNMP SNMPv2 Communities SNMPv3 Users SNMPv3 View
Notifications	Alarms Alarm Config Syslog
Maintenance	Backup Restore Save startup-config Factory Defaults Firmware Update Reboot
ConsoleFlow	Status, Configuration, Connection 1 and 2
Lantronix Provision Manager	Configuration, Status

Webpage Controls and Messages

Web timeout: The timeout is set to 10 minutes and is not currently configurable.



Help icon: click to display this manual on the Lantronix web site. A future release will display context-sensitive help.



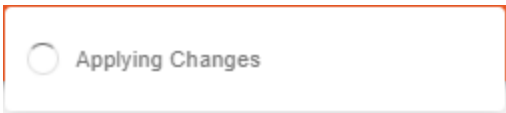
Logout icon: click to log out of the switch user interface; the Login page displays.

Page-specific controls: Typically these affect some portion of data on the current page, such as adding or deleting a table entry. For example, on the `Add Logical Interface` button on the System > IP Settings page click the button to add a row to the IP Settings table.

Apply: Click to save webpage settings to running-config.

Cancel: Click to cancel webpage settings.

Pop-up messages :These widgets are pop-up messages showing progress of a request or results from a response. Pop-up messages clear automatically after displaying for about 5 seconds:



Applying changes: Wait for the changes to be applied then continue.



The changes were successfully applied; continue operation.



The changes were not applied; retry the operation.

Error Logging in. Failed to fetch: The Sign-in attempt failed. Click the OK button to clear the message, re-enter the correct Username and Password, then continue operation. If the message displays again, contact your network administrator.

System

This menu section lets you set and view system-level parameters such as System, IP, Static Routes, ARP, NTP, Diagnostics, and DHCP.

System > System Info

The System Info page lets you set and view System-level parameters. This is the startup page that displays after a successful Login.

The screenshot shows the Lantronix System Info page. The page has a header with the Lantronix logo and the title 'System Info'. Below the header is a sidebar with navigation options: System, Port Management, PoE Management, SNMP, Notifications, Maintenance, ConsoleFlow, and Lantronix Provision Manager. The main content area is divided into three sections: System Config, System Time, and Version Info.

System Config:

System Name LSS2200-8P	System Contact
System Location	Banner --: EOS :--

System Time:

Note: Changing the system time will require relogging in.

System Date 04/19/2023	System Time 12:22 AM	System Timezone UTC
---------------------------	-------------------------	------------------------

Version Info:

Hardware Rev DAB	MAC Address 00:C0:F2:96:08:C0
Serial Number 00C0F29608C0	Firmware Version 1.7.0.0R5

Parameter descriptions:

System Config:

System Name: Enter a specific name for the switch system or use the default system name (*LSS220-8P*). The field accepts both '_' (underscore) and '.' (period or dot character), but no space character.

System Contact: Enter any desired contact information; the default is blank. The field accepts '_' (underscore) character, the '.' (period or dot character), and space character.

System Location: Enter some location information; the default is blank. The field accepts '_' (underscore) character, the '.' (period or dot character), and space character.

Banner: Enter a CLI login banner message for the switch system or use the default banner (*--: EOS :--*).

System Time: Note: Changing the system date or time will require relogging in.

System Date: Enter a system date or click the icon and select one. The format is *mm/dd/yyyy*.

System Time: Enter a system time or click the icon and select one. The format is *hh:mm AM* or *PM*. **Note** that changing the System Time requires logging in to the Web UI or REST API clients again. Changing system time does not affect open CLI sessions. Changing system time manually via any interface may cause open Web UI and REST API client sessions to close because they use a time-dependent web token. The default is UTC. Universal Time Coordinated / Universal Coordinated Time is the successor to Greenwich Mean Time (GMT).

System Timezone: Select a specific Timezone at the dropdown or use the default Timezone (*UTC*). **Note:** NTP is set to on by default (for ConsoleFlow). You must manually set the Timezone. See [System > NTP](#) on page 20.
Note: Changing the system time will require relogging in.

Version Info:

Hardware Rev: Displays the switch hardware version (e.g., *DAB*).

MAC Address: Displays the switch MAC address in the format *11:22:33:44:55:66*.

Serial Number: Displays the serial number assigned to this switch. The serial number is the last 12 digits of the switch MAC address (e.g., *00C0F29600B0*).

Firmware Version: Displays the current switch firmware version (e.g., *1.7.0.0R5*).

CPU: Displays current CPU usage as a percentage (*Current, 5 mins, and 15 minute* increments).

The screenshot shows the 'System Info' page in the Lantronix web interface. The left sidebar contains a navigation menu with items like IP Settings, IP Status, IP Statistics, Static Routes, ARP, NTP, Diagnostics, DHCP Relay, DHCP Server, DHCP Snooping, BLE, Manage Users, Port Management, PoE Management, SNMP, and Notifications. The main content area is divided into several sections: CPU usage (Current: 14.78%, 5 mins: 15.36%, 15 mins: 15.17%), Memory (Total: 912.875 MB, Available: 327.160 MB), Temperature (CPU: 48.92 C), Power (Voltage: 55.63 V, Current: 0.08 A, Power: 4.45 W), and Telnet (Enabled). A warning message is displayed for Telnet: 'Warning: Non-secure Telnet State is enabled. Device is vulnerable to Cleartext Transmission of Sensitive Information. Setup and verify SSH, then disable Telnet.' An 'Apply' button is located at the bottom right of the main content area. The footer of the page reads 'Copyright © 2022 Lantronix Inc. All rights reserved.'

Memory:

Total Memory: Displays the total memory currently used in MB.

Available Memory: Displays the total available memory in MB (e.g., *416.602 MB*).

Temperature: Displays the temperature of the switch CPU (in °C).

Power: Displays the existing voltage in Volts, current in Amps, and power in `Watts.

Telnet: At the dropdown select *Enabled* to enable Telnet operation. The default is Telnet operation *Disabled*. When you select Enabled, a message displays: *Warning: Non-secure Telnet State is enabled. Device is vulnerable to Cleartext Transmission of Sensitive Information. Setup and verify SSH, then disable Telnet.*

Buttons:

Apply: Click to save webpage settings to running-config.

Messages:

409 Error: Cannot set local time with clock source set to NTP

Note: Changing the system time will require relogging in.

Data not available

System > IP Settings

The IP Settings page lets you set and view IP parameters. By default, this page displays one VLAN (*VLAN1*).

Note: The IP Settings page shows only configured IP addresses. IP addresses received from a DHCP server are displayed on the “IP Status” web page. The initial IP Settings page is shown below.

Interface	Protocol	IPv4 Address	IPv4 Netmask	DNS	Delete
VLAN1	Static	192.168.60.1	255.255.255.0		

Parameter descriptions:

Interface: Displays the name of a configured VLAN interface (*VLAN1*).

Protocol: At the dropdown select the protocol to use for the VLAN1 interface:

none: Do not use a protocol for VLAN1.

Static: Use a static protocol for VLAN1. The default is *Static*. Make this VLAN a static VLAN. A static VLAN is a group of ports designated by the switch as belonging to the same broadcast domain (i.e., all ports carrying traffic for a specific subnet address belong to the same VLAN). Using a static VLAN lets you group users by logical function instead of by physical location. This is a widely used method due to small administration overhead and security.

DHCP: Use DHCP for VLAN1. This selection lets you configure multiple DHCP pools on the DHCP server and assign a DHCP pool to each VLAN. The VLAN ID is automatically determined using DHCP Option 43 (Vendor Specific Info).

Protocol

- none
- Static
- DHCP

IPv4 Address: Enter a valid IPv4 address.

IPv4 Netmask: Enter a valid IPv4 netmask.

DNS: Enter a valid DNS server name or IP address. The “DNS” field takes a list of zero or more IP addresses. Examples: [] or ["192.168.11.2"] or ["192.168.60.101", "192.168.11.2"] . In the Web UI you must enclose the DNS value in square brackets for the request.

Delete: Click the icon to remove the unsaved entry from the table.

Buttons:

Cancel: Click to cancel webpage settings.

Add Logical Interface: Click to add a row to the IP Settings table.

Apply: Click to save webpage settings to running-config.

Messages:

409 Error: Configured IP Network (192.168.60.1/255.255.255.0) conflicts with existing network on interface VLAN 1.

Adding a VLAN

Click the Add Logical Interface button to add and configure another VLAN on the New Logical Port Config page:

The screenshot shows the 'New Logical Port Config' page in the Lantronix web interface. The left sidebar lists navigation options: System, System Info, IP Settings, IP Status, IP Statistics, Static Routes, ARP, NTP, Diagnostics, and DHCP Relay. The main content area is titled 'New Logical Port Config' and contains a form with the following fields:

- VLAN: 1
- Protocol: Static (dropdown menu)
- IPv4 Address: (text input)
- IPv4 Netmask: (text input)
- DNS: (text input)

At the bottom right of the form are 'Cancel' and 'Apply' buttons. The footer of the page reads 'Copyright © 2023 Lantronix Inc. All rights reserved.'

Parameter descriptions:

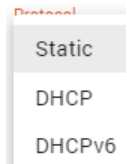
VLAN: Select a VLAN ID in the range of 2-4094.

Protocol: At the dropdown select the desired protocol for this VLAN:

Static: Make this VLAN a static VLAN. A static VLAN is a group of ports designated by the switch as belonging to the same broadcast domain (i.e., all ports carrying traffic for a specific subnet address belong to the same VLAN). Using a static VLAN lets you group users by logical function instead of by physical location. This is a widely used method due to small administration overhead and security. This is the default setting.

DHCP: Use DHCPv4 as the protocol for this VLAN. This selection lets you configure multiple DHCP pools on the DHCP server and assign a DHCP pool to each VLAN. The VLAN ID is automatically determined using DHCP Option 43 (Vendor Specific Info).

DHCPv6: Use DHCPv6 as the protocol for this VLAN. This selection works by inserting DHCPv6 Interface-ID Option (Option 18) in DHCPv6 packets.




IPv4 Address: Enter a valid IPv4 address.

IPv4 Netmask: Enter a valid IPv4 netmask.

DNS: Enter a valid DNS server name or IP address.

Message: 409 Error: Configured IP Network (192.168.60.1/255.255.255.0) conflicts with existing network on interface VLAN 1.

Deleting a VLAN

Delete: Click the  icon in the Delete column of a row to delete the instance from the table and the system.

System > IP Status

The IP Status page displays current switch Internet Protocol status information. The IP Status fields are read-only.

The screenshot shows the Lantronix web interface for the LSS2200-8P switch. The left sidebar contains a navigation menu with items: System Info, IP Settings, IP Status (highlighted), IP Statistics, and Static Routes. The main content area is titled 'IP Status' and features a table with the following data:

Port Name	IP Address	Network Mask	MTU	State	MAC Address
VLAN1	192.168.60.1	255.255.255.0	10240	UP	00:C0:F2:96:08
VLAN10	172.168.60.1	255.255.254.0	10240	UP	00:C0:F2:96:08

Copyright © 2023 Lantronix Inc. All rights reserved.

Parameter descriptions:

Port Name: Displays the name of the port; *VLAN 1* by default.

IP Address: Displays the IP address (e.g., *192.168.10.50*).

Network Mask: Displays the network mask (e.g., *255.255.255.0*).

MTU: Displays the maximum transmission unit (e.g., *10240* bytes).

State: Displays the operational state (*UP* or *DOWN*)

MAC Address: Displays the MAC address in the format *11:22:33:44:55:66*.

System > IP Statistics

The IP Statistics page displays the current Internet Protocol statistics. The IP statistics fields are read-only.

The screenshot shows the Lantronix web interface for IP Statistics. The page title is 'IP Statistics'. The left sidebar contains the following menu items: LSS2200-8P, System, System Info, IP Settings, IP Status, IP Statistics (selected), Static Routes, and ARP. The main content area displays a table with the following data:

Name	Direction	Bytes	Packets	Multicast	Errors	Dropped	Overrun
VLAN1	Rx	526222	3385	1219	0	17	0
	Tx	526222	3385	N/A	0	17	N/A
VLAN2	Rx	0	0	0	0	0	0
	Tx	0	0	N/A	0	0	N/A

Copyright © 2023 Lantronix Inc. All rights reserved.

Parameter descriptions:

Name: Displays the assigned port name (e.g., *VLAN1*).

Direction: Displays whether the direction is Receive (*Rx*) or Transmit (*Tx*).

Bytes: Displays the number of bytes received or transmitted.

Packets: Displays the number of packets received or transmitted.

Multicast: Displays the number of multicast packets received or transmitted.

Errors: Displays the number of errored packets received or transmitted.

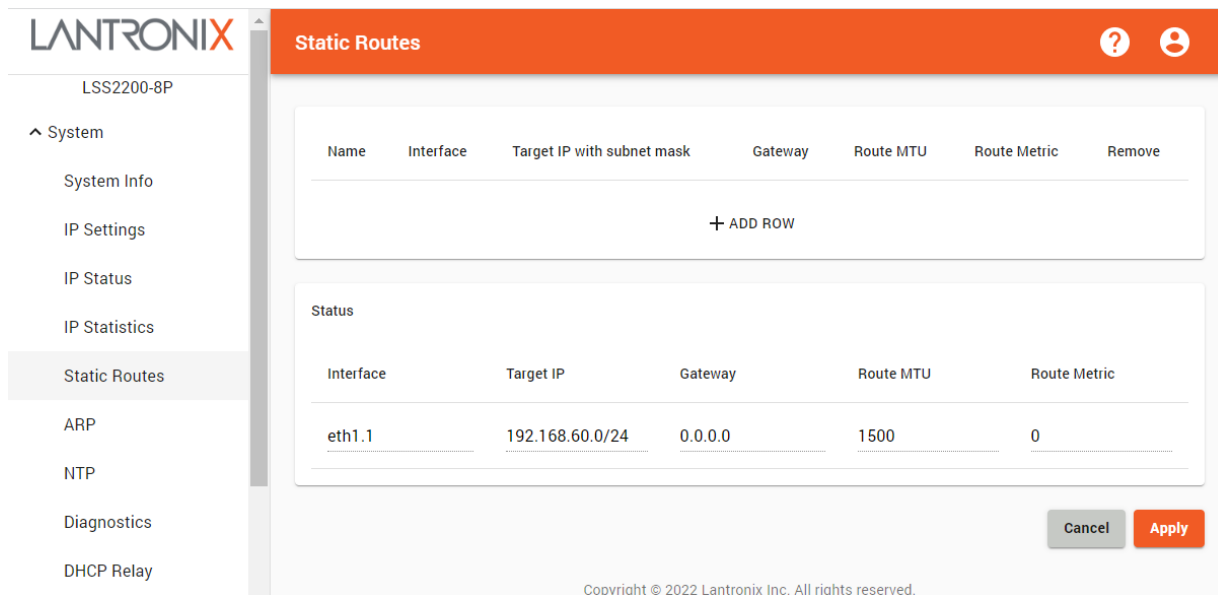
Dropped: Displays the number of dropped packets received or transmitted.

Overrun: Displays the number of overrun packets received or transmitted.

System > Static Routes

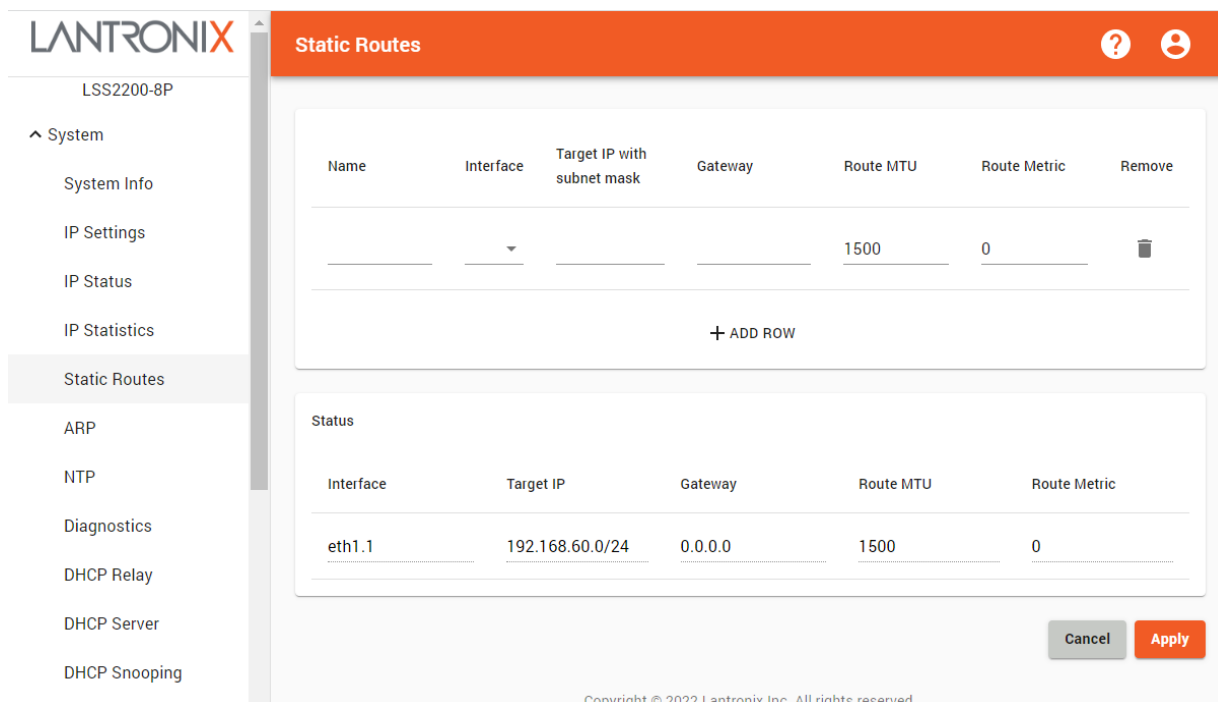
This page lets you enter new or view existing Static Routes. A static route is a pre-determined pathway that a packet must travel to reach a specific host or network. Static routing uses a manually-configured routing entry instead of information from dynamic routing traffic.

The static routing table is defined by configuration. Each entry specifies the addresses to route (IP address and subnet), the IP address of the next hop gateway and a metric. The route is selected by finding the most specific matching route in the table (longest prefix match). If there are routes that are equally specific, the one with the lowest metric is chosen.



Adding a Static Route

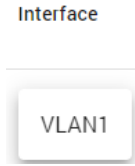
Click the + ADD ROW icon to display a new row to configure a new Static Route:



Parameter descriptions:

Name: Enter a name for the new Static Route to be added.

Interface: Enter a new Static Route interface or view an existing Static Route interface (e.g., VLAN1).




Target IP with subnet mask: Enter a new Static Route target IP address or view an existing Static Route target IP address (e.g., 192.168.10.0/24).

Gateway: Enter a new Gateway IP address or view an existing Gateway IP address in the format 0.0.0.0.

Route MTU: Enter a new or view an existing Route Maximum Transmission Units. This is the size of the largest protocol data unit (PDU) that can be communicated in one network layer transaction. The switch supports up to 10,240 byte packets.

Route Metric: Indicates the cost of a route. If multiple routes exist to a given destination network ID, the route metric decides which route is to be taken. The route with the lowest metric is the preferred route.

Remove: Click the  icon in the Remove column of a row to delete the instance from the table and the system.

Buttons:

Cancel: Click to cancel webpage settings.

Apply: Click to save webpage settings to running-config.

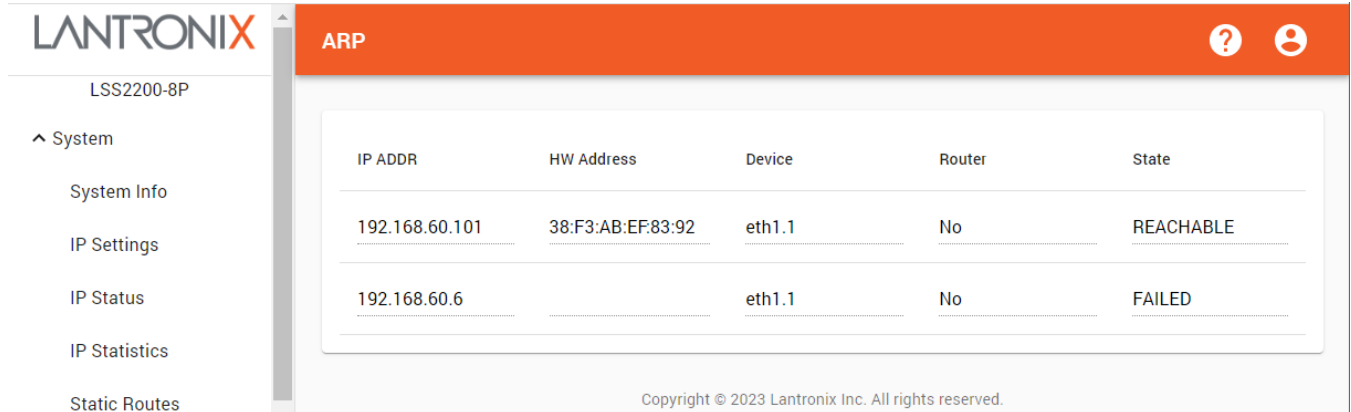
Deleting a Static Route

Only routes that were added manually can be deleted. Routes that are automatically created when creating a VLAN cannot be deleted manually; they are deleted when the VLAN is deleted.

System > ARP

The Address Resolution Protocol page displays current ARP parameters. ARP is a layer 2 protocol used to map MAC addresses to IP addresses. The fields are read-only.

The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address. This mapping is a critical function in the Internet Protocol suite.



Parameter descriptions:

IP ADDR: Displays the current switch IP address (e.g., *192.168.10.99*).

HW Address: The discovered hardware (MAC) address in the format *11:22:33:44:55:66*.

Device: The device name of the local switch interface reporting this ARP entry (e.g., *eth1.1*).

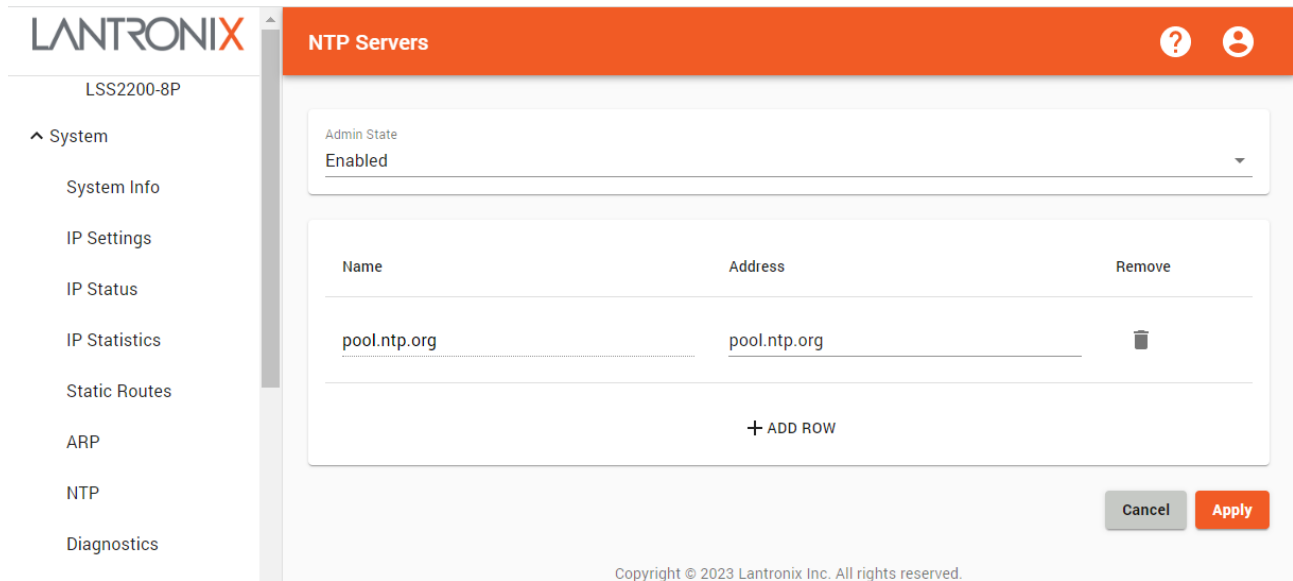
Router: Indicates whether the discovered device is a router (*Yes* or *No*).

State: Displays the current ARP state (e.g., *REACHABLE*, *DELAY*, *STALE*). ARP states are listed and described below.

ARP Cache Entry State	Meaning
PERMANENT	Never expires; never verified
NOARP	Normal expiration; never verified
REACHABLE	Normal expiration
STALE	Still usable; needs verification
DELAY	Schedule ARP request; needs verification
PROBE	Sending ARP request
INCOMPLETE	First ARP request sent
FAILED	No response received

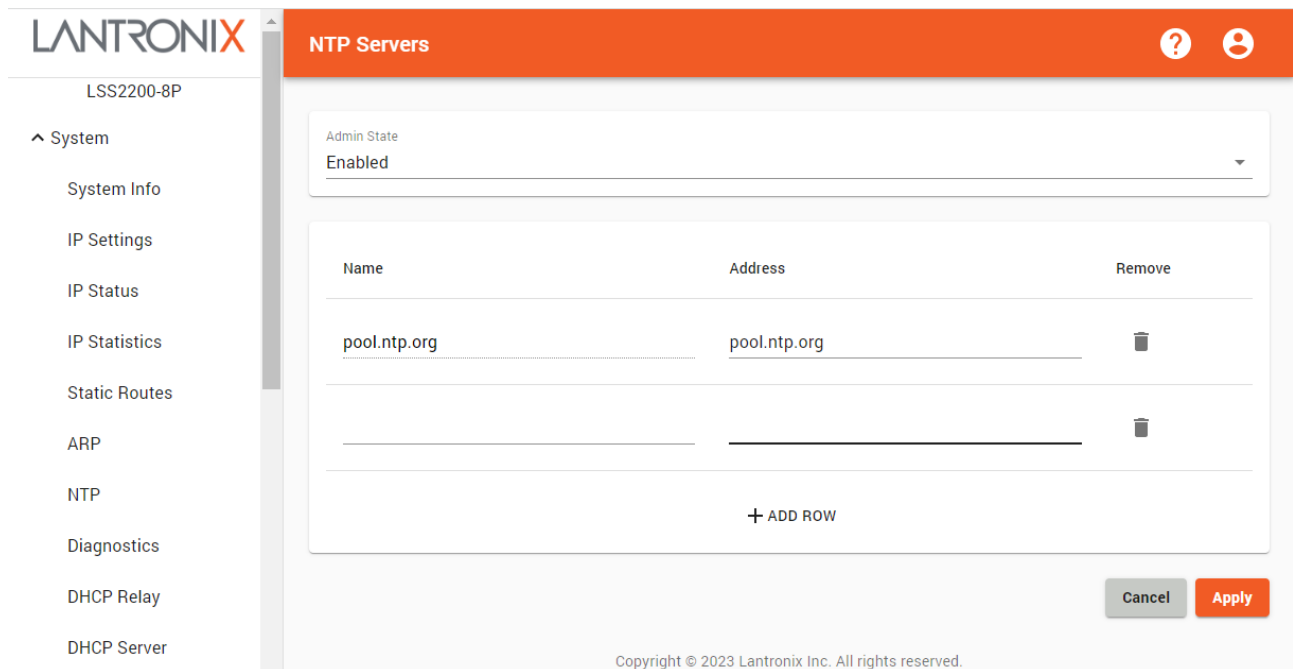
System > NTP

The NTP page lets you view and set Network Timing Protocol parameters. NTP is an internet protocol used to synchronize with computer clock time sources in a network. **Note:** NTP is set to 'On' by default (for ConsoleFlow). You must manually set the Timezone on the System Info page.



Adding an NTP Server

Click the + ADD ROW icon to display a new row to configure a new NTP Server:




Parameter descriptions:

Name: The name of the organization providing the NTP service (e.g., pool.ntp.org).

Address: The IP address or domain name of the NTP service.

Deleting an NTP Server

Remove: Click the  icon in the Remove column of a row to delete the instance from the table and the system.

Buttons:

Cancel: Click to cancel webpage settings.

Apply: Click to save webpage settings to running-config.

System > Diagnostics

The Diagnostics page provides access to Ping, NS Lookup, and Traceroute functions.

The screenshot displays the Lantronix web interface for the LSS2200-8P device. The top navigation bar is orange and contains the 'Diagnostics' title, a help icon, and a user profile icon. The left sidebar lists various system settings, with 'Diagnostics' highlighted. The main content area is divided into three sections: 'Ping', 'NS Lookup', and 'Traceroute'. Each section has input fields for 'Host' and 'Interface', and a 'Count' field (set to 5 for Ping). Action buttons for 'Ping', 'NS Lookup', and 'Trace Route' are located at the bottom right of each section. A 'Clear' button is positioned at the bottom right of the entire diagnostics area. The browser address bar at the bottom left shows the URL 'https://172.27.100.32/diagnostics'.

Ping parameters:

Host: Enter the ping host IP address or Fully Qualified Domain Name.

Interface: Select an interface to be pinged.

Count: Select the number of pings to be sent.

Ping: Click the Ping button to begin the Ping process.

Sample Ping output:

```
PING 192.168.60.1 (192.168.60.1) from 192.168.60.1: 56 data bytes
64 bytes from 192.168.60.1: seq=0 ttl=64 time=0.232 ms
64 bytes from 192.168.60.1: seq=1 ttl=64 time=0.244 ms
```

```
--- 192.168.60.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.232/0.238/0.244 ms
```

Ping Messages:

ping: can't set multicast source interface

ping: bad address 'undefined'

ping: bad address 'BobB'

NS Lookup parameters:

Host: Enter the nslookup host IP address or Fully Qualified Domain Name.

NS Lookup: Click the NS Lookup button to begin the Name Server Lookup process.

Messages: **** Can't find BobB: No answer*

Traceroute parameters:

Host: Enter the Traceroute host IP address or Fully Qualified Domain Name.

Interface: Enter an interface to be traced. This must be a VLAN interface (e.g., VLAN100).

Traceroute: Click the Traceroute button to begin the traceroute process.

Messages: *traceroute: can't bind to interface G1/1: No such device*

Buttons:

Clear: Click to clear the results of the previous operation(s). The switch caches results from each operation so they can be polled. Results must be cleared before the same operation can be run again.

Sample traceroute output:

```
traceroute: can't bind to interface vlan1: No such device
traceroute to 192.168.60.1 (192.168.60.1), 30 hops max, 46 byte packets
 1 192.168.60.1 (192.168.60.1) 0.037 ms 0.019 ms 0.011 ms
```

System > DHCP Relay

The DHCP Relay page lets you enable and configure DHCP Relay parameters. A DHCP relay agent is a host or router that forwards DHCP packets between clients and servers when the server is on a different network.

The screenshot shows the Lantronix web interface for the DHCP Relay configuration page. The interface includes a sidebar on the left with the following menu items: System, System Info, IP Settings, IP Status, IP Statistics, Static Routes, ARP, NTP, Diagnostics, and DHCP Relay. The main content area is titled 'DHCP Relay' and contains the following configuration fields:

- Enabled:** A dropdown menu currently set to 'Disabled'.
- Relay Address:** A text input field.
- Relay Interface:** A text input field.
- Server Address:** A text input field.
- Server Interface:** A text input field.

At the bottom right of the configuration area, there are two buttons: 'Cancel' and 'Apply'. The footer of the page reads 'Copyright © 2023 Lantronix Inc. All rights reserved.'

Parameter descriptions:

Enabled: At the dropdown select Enabled. The default is DHCP Relay disabled.

Relay Address: Enter the DHCP Relay address or FQDN (Fully Qualified Domain Name).

Relay Interface: Enter the DHCP Relay interface.

Server Address: Enter the DHCP Relay server IP address. or FQDN (Fully Qualified Domain Name).

Server Interface: Enter the DHCP Relay server interface.

Buttons:

Cancel: Click to ignore any webpage changes.

Apply: Click to save webpage settings to running-config.

Messages:

400 Error: Input payload validation failed

409 Error: Invalid input – Interface AAAA does not exist

RLYINTERFACE: 'G1/1' does not match '[A-Z][A-Z0-9_](1.13)[A-Z0-9]'

SRVINTERFACE: 'G1/3' does not match '[A-Z][A-Z0-9_](1.13)[A-Z0-9]'

System > DHCP Server

Adding a DHCP Server

The DHCP Server page lets you view and set basic and advanced DHCP server parameters.

The IPv4 address for the switch can be obtained via DHCP Server for VLAN 1. To manually configure an IP address, you must change the switch's default settings to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment.

On the default page, click the **+ ADD ROW** icon to display a new page to configure a new DHCP Server:

The screenshot shows the Lantronix web interface for configuring a DHCP server. The left sidebar lists various system settings, with 'DHCP Server' selected. The main configuration area includes:

- Input fields for 'Server Name' and 'Domain Name'.
- A table for 'Listen Addresses' with columns for 'Authoritative', 'Duration', and 'Units', and a '+ ADD ROW' button.
- A 'Ranges Table' with columns for 'Start IP Address', 'End IP Address', 'Netmask', 'Broadcast', 'Vendor Class Identifier', 'User Class Identifier', 'Duration', 'Units', and 'Remove', and a '+ ADD ROW' button.
- Sections for 'Default Router', 'DNS Servers', and 'NTP Servers', each with a '+ ADD ROW' button.
- A 'Show Advanced Settings' button.
- 'Cancel' and 'Apply' buttons at the bottom right.
- A copyright notice: 'Copyright © 2023 Lantronix Inc. All rights reserved.'

Parameter descriptions:

Server Name: Enter the name of the DHCP server.


Domain Name: Enter the domain name for the DHCP server.

Authoritative: At the dropdown select *Enabled* or *Disabled*. With a DHCP server configured as authoritative, the server will respond with DHCP ACK or NACK as appropriate for all the received DHCP REQUEST and DHCP INFORM packets belonging to the subnet. Non-authoritative DHCP INFORM packets received from the clients on a non-authoritative pool will be ignored.


Duration: DHCP Lease Time; the amount of time that a network device can use an IP Address in a network.

Units: At the dropdown select *Days*, *Hours* or *Minutes* as the unit of measure for the Duration parameter.

Listen Address: Enter the valid IPv4 IP address of the "listener". A DHCP server listens to UDP port 67 and dynamically assigns IP addresses and other network parameters to DHCP clients.

Remove: Click the  icon in the Remove column of a row to delete the instance from the table and the system.

Ranges Table: Click the **+ ADD ROW** icon to display a new row to configure DHCP server range parameters:

Start IP Address	End IP Address	Netmask	Broadcast	Vendor Class Identifier	User Class Identifier	Duration	Units	Remove
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="Days"/>	
+ ADD ROW								

Start IP Address: Enter a valid IPv4 starting IP address.

End IP Address: Enter a valid IPv4 ending IP address.

Netmask: Enter a valid IPv4 netmask.


Broadcast: Enter the broadcast DHCP server IP address.

Vendor Class Identifier: Enter the class identifier option to be used by DHCP clients to identify the type and configuration of a DHCP client. Vendor Classes typically assign vendor-specific options to clients that share a common vendor type.




User Class Identifier: A DHCP client class is a common way to differentiate and classify devices on your network based on specific configuration criteria. This classification lets you assign a specific configuration of DHCP options to any subset of DHCP clients you define. User Classes assign DHCP options to a group of clients that require similar configuration.

Duration: DHCP Lease Time; enter the amount of time that a network device can use an IP Address in a network (e.g., 4 days, 3 hours, or 2 minutes).

Units: At the dropdown select *Days* (0-365), *Hours* (0-365) or *Minutes* (0-365) as the unit of measure for the Duration parameter.

Remove: Click the  icon in the Remove column of a row to delete the instance from the table and the system.


Router / DNS / NTP Table: Click the + ADD ROW icon to display a new row to configure additional parameters:

Default Router	Remove	DNS Servers	Remove	NTP Servers	Remove
<input type="text"/>		<input type="text"/>		<input type="text"/>	
<input type="button" value="+ ADD ROW"/>		<input type="button" value="+ ADD ROW"/>		<input type="button" value="+ ADD ROW"/>	


Default Router: Enter the default router IP address (optional).

Remove: Click the  icon in the Remove column of a row to delete the instance.

DNS Servers: Enter one or more DNS server IP addresses (optional).

Remove: Click the  icon in the Remove column of a row to delete the instance.

NTP Servers: Enter one or more NTP server IP address(es) (optional).

Remove: Click the  icon in the Remove column of a row to delete the instance.

Buttons:

Cancel: Click to cancel webpage settings.

Apply: Click to save webpage settings to running-config.

Messages:

400 Error: Input payload validation failed

400 Error: Invalid input – DHCP Server undefined already exists

RLYINTERFACE: 'G1/1' does not match '[A-Z][A-Z0-9_]{1.13}[A-Z0-9]'

SRVINTERFACE: 'G1/3' does not match '[A-Z][A-Z0-9_]{1.13}[A-Z0-9]'

DHCP Server Advanced Settings

Show Advanced Settings: Click to display additional DHCP Server sections and parameters (shown below).

Hide Advanced Settings: Click to hide the additional DHCP Server sections and parameters.

Parameter descriptions:

Client ID Table: Click the + ADD ROW icon to display client ID parameters to configure:


Client ID: Enter the client ID.

IP Address: Enter a valid IPv4 IP address.

Hostname: Enter the host name or a valid IPv4 IP address.

Duration: Enter or select the desired lease duration (0-365).

Units: At the dropdown select the units of measure to use (*Days, Hours, or Minutes*).

Remove: Click the  icon in the Remove column of a row to delete the instance.

Host MAC Table: Click the + ADD ROW icon to display Host MAC parameters to configure:

MAC Address: Enter a MAC address in the format 11:22:33:44:55:66).

IP Address: Enter a valid IPv4 IP address.

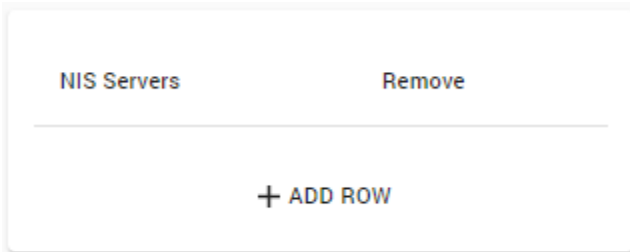
Hostname: Enter the host name or a valid IPv4 IP address.

Duration: Enter or select the desired lease duration (0-365).

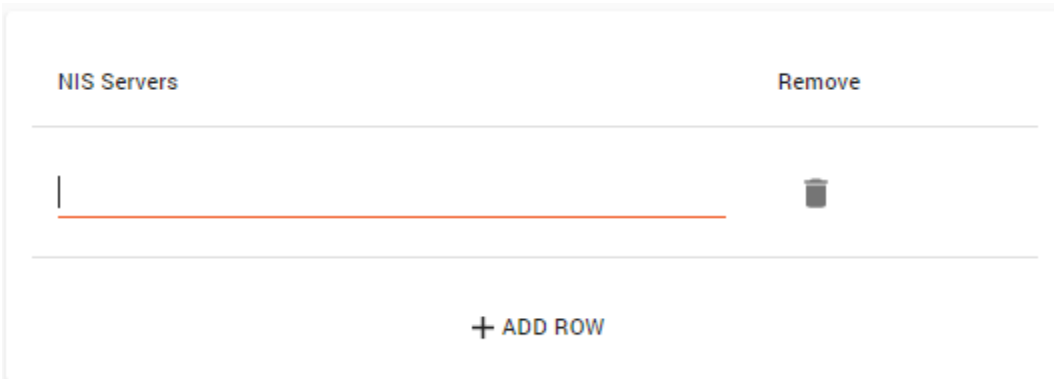
Units: At the dropdown select the units of measure to use (*Days, Hours, or Minutes*).

Remove: Click the  icon in the Remove column of a row to delete the instance.

NIS Servers:



Click the + ADD ROW icon to display a new row to configure additional parameters:



NIS Servers: Enter a valid IPv4 IP address.

Remove: Click the  icon in the Remove column of a row to delete the instance.

NetBIOS table: Click the + ADD ROW icon to display a new row to configure additional parameters:

The screenshot displays a configuration interface for NetBIOS. At the top, there is a table titled 'NetBIOS Name Servers' with a 'Remove' column and a '+ ADD ROW' button. Below the table, there are three input fields: 'NIS Domain Name', 'NetBIOS Scope', and 'NetBIOS Node Type' (a dropdown menu).

NetBIOS Name Servers: Enter a valid NetBIOS Name Server in IPv4 format.

NIS Domain Name: Enter a valid IPv4 IP address.

NetBIOS Scope: The NetBIOS scope identifier sets the NetBIOS domain. Only users with equivalent scope identifiers can communicate with each other.

NetBIOS Node Type: At the dropdown select one of the four node types:


Broadcast: b-node: broadcast of the name asking for IP.

Peer-to-Peer: p-node: peer-to-peer using NBNS (NetBIOS Name Service) such as WINS (Windows Internet Name Service).

Mixed: m-node: mix of b and p, defaults to b-node, if that fails uses p-node resolution.

Hybrid: h-node: hybrid of b and p, defaults to p-node, if that fails uses b-node resolution.

The screenshot shows a dropdown menu for 'NetBIOS Node Type' with four options: Broadcast, Peer-to-Peer, Mixed, and Hybrid.

Remove: Click the  icon in the Remove column of a row to delete the instance.

NIS Server IP Address: Enter a valid IPv4 IP address.

Remove: Click the  icon in the Remove column of a row to delete the instance.

Microsoft DHCP client using NetBIOS


A Microsoft DHCP client using the NetBIOS protocol must contact a WINS server for name resolution. A WINS server is a Microsoft Windows-based server running the Windows Internet Name Service (WINS) that can accept NetBIOS name registrations and queries. How WINS works on a network is determined by the node type set for a client. The node type defines how name services work. WINS clients can be one of four node types:



- **B-Node (Broadcast Node):** Broadcast messages are used to register and resolve names. Computers that need to resolve a name broadcast a message to every host on the local network, requesting the IP address for a computer name. Best for small networks.
- **P-Node (Peer-to-Peer Node):** WINS servers are used to register and resolve computer names to Internet Protocol (IP) addresses. Computers that need to resolve a name send a query message to the server and the server responds. Best if you want to eliminate broadcasts. In some cases, however, resources might not be seen as available if the WINS server isn't updated by the computer providing the resources.
- **M-Node (Mixed Node):** A combination of B-Node and P-Node. WINS clients first try to use broadcasts for name resolution. If this fails, the clients then try using a WINS server. Still means much broadcast traffic.
- **H-Node (Hybrid Node):** A combination of B-Node and P-Node. WINS clients first try to use a WINS server for name resolution. If this fails, the clients then try broadcasts for name resolution. Best for most networks that use WINS servers because it reduces broadcast traffic.

Options table: Click the + ADD ROW icon to display a new row to configure DHCP option parameters (shown below left):

Option Number: Enter the desired DHCP option number.

Option Value: Enter the desired DHCP option value.

Remove: Click the  icon in the Remove column of a row to delete the instance.

Options			Vendor		
Option Number	Option Value	Remove	Vendor Class ID	Value	Remove
1					
+ ADD ROW			+ ADD ROW		

Vendor table: Click the + ADD ROW icon to display a new row to configure DHCP vendor parameters (shown above right):

Vendor Class ID: Enter the desired DHCP vendor class identifier. Using the vendor class identifier allows DHCP administrators to assign vendor-specific DHCP options to devices without running the risk of duplicating options within the DHCP scope. For example, it allows an organization to supply separate DHCP option 43 values to different vendor devices.

Value: Enter the desired DHCP vendor class value. See the IANA [DHCP Options](https://www.iana.org/assignments/dhcp-extensions/) webpage.

Remove: Click the  icon in the Remove column of a row to delete the instance.

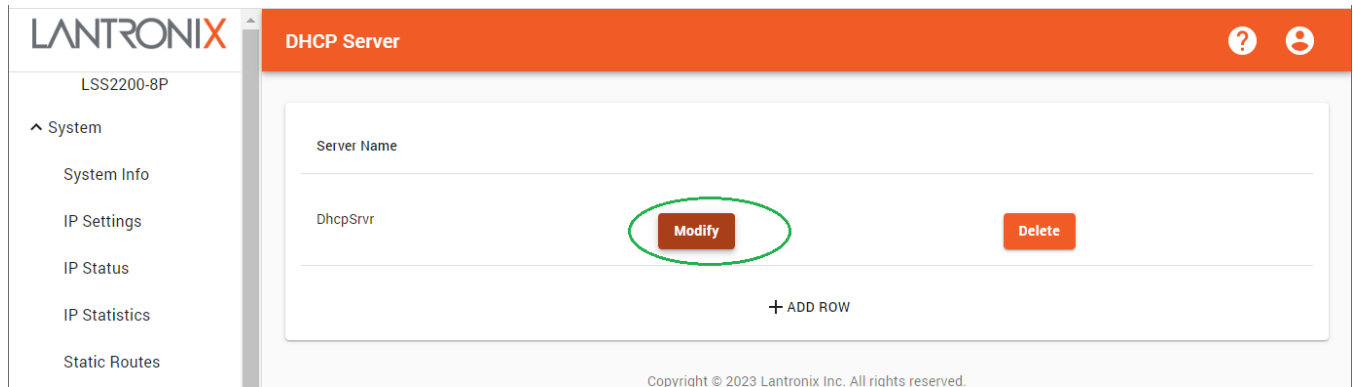
Buttons:

Cancel: Click to cancel webpage settings.

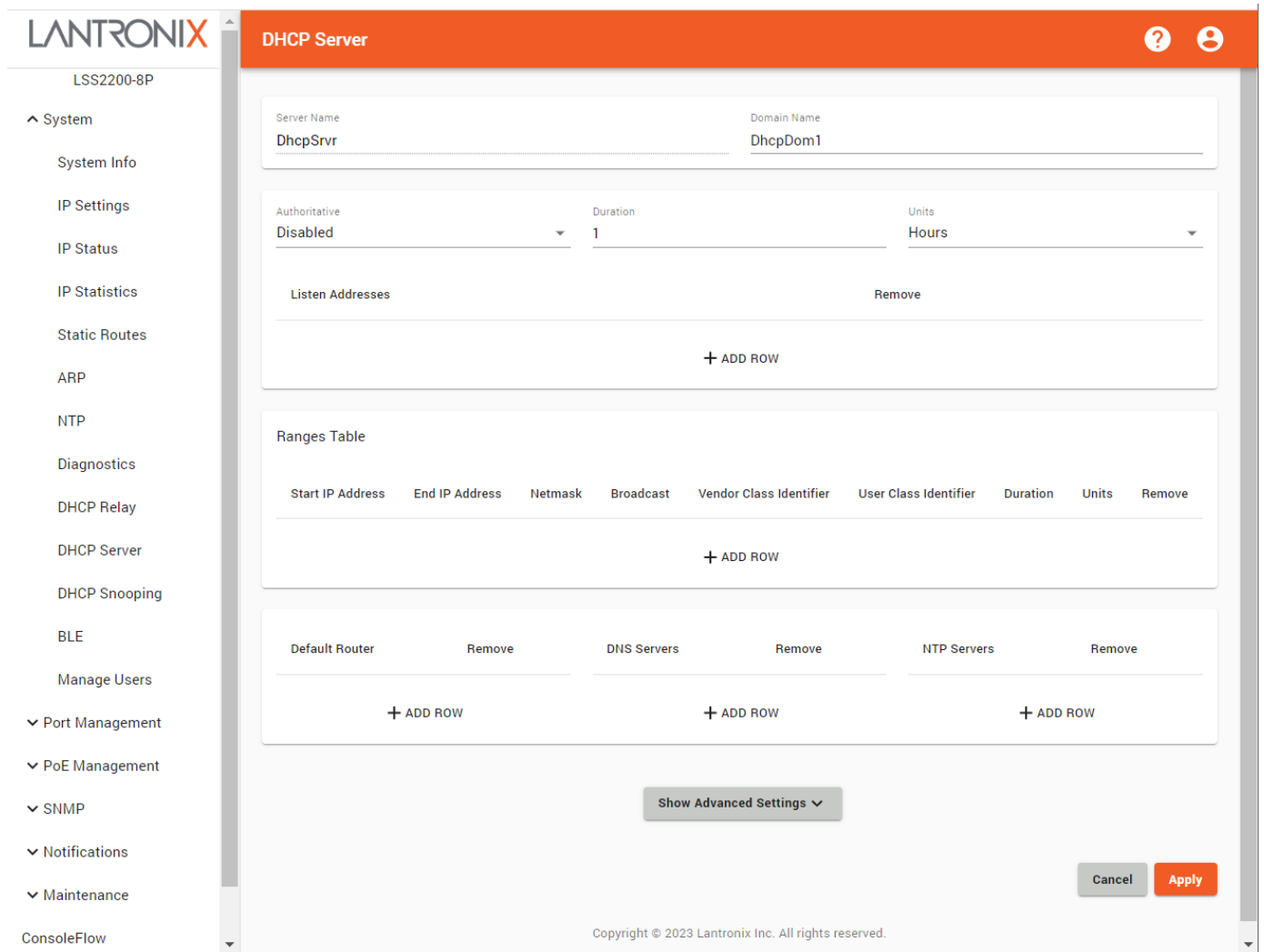
Apply: Click to save webpage settings to running-config.

Modify an Existing DHCP Server

1. At the DHCP Server page click the Modify button:



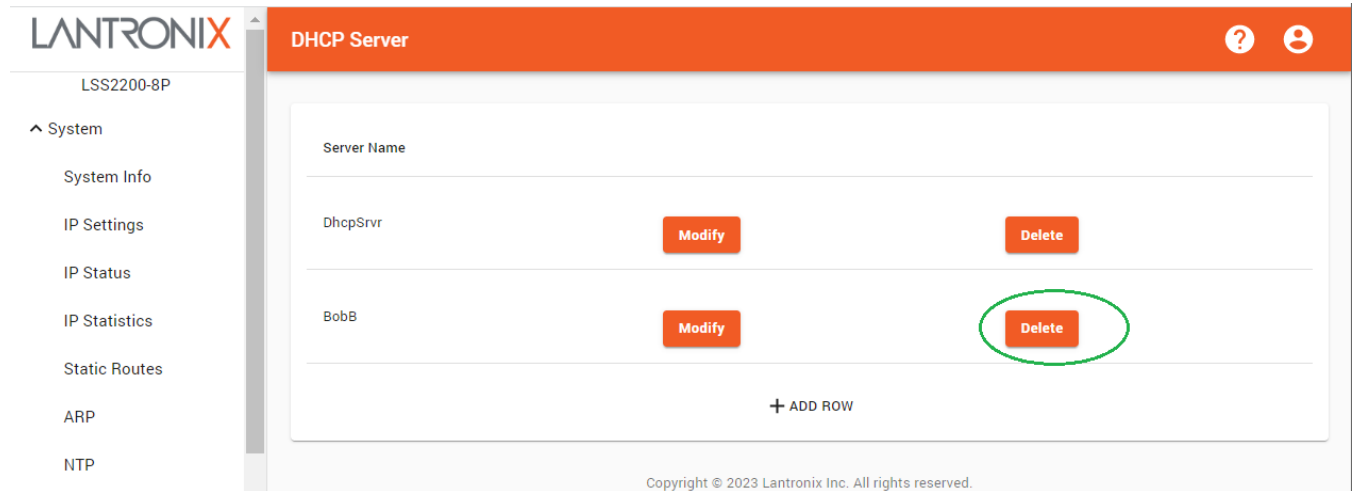
2. Modify the desired parameters. See above for parameter descriptions.



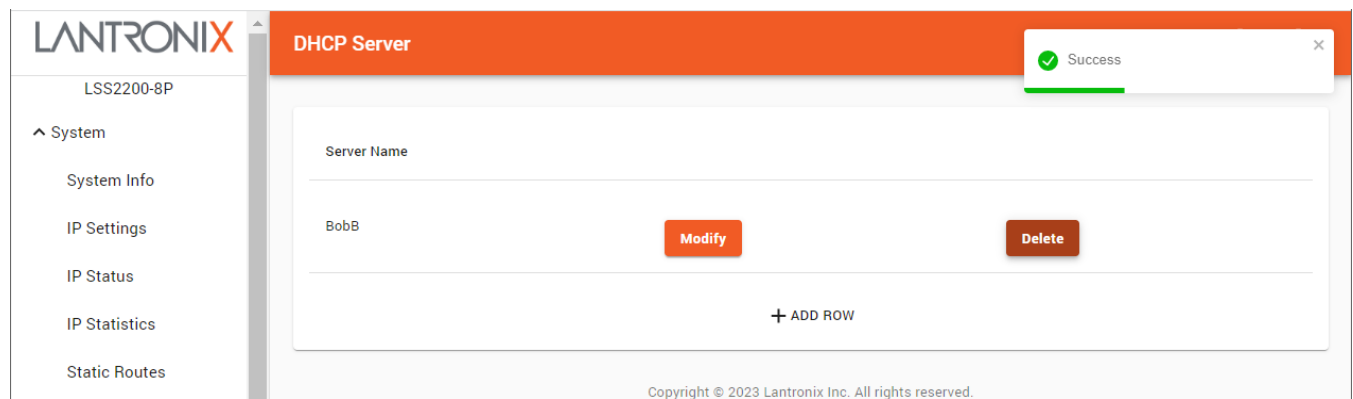
3. Click the Apply button when done.

Delete an Existing DHCP Server

1. At the DHCP Server page click the Delete button:



2. Wait for the delete process to successfully complete:



System > DHCP Snooping

The DHCP Snooping page lets you globally enable and disable DHCP snooping, and also configure each switch port as Trusted or Untrusted. DHCP Snooping is disabled by default, and all switch ports are set to 'Untrusted' by default.

DHCP snooping is a series of techniques applied to improve the security of a DHCP infrastructure. DHCP servers allocate IP addresses to clients on a LAN. DHCP snooping can be configured on LAN switches to exclude rogue DHCP servers and remove malicious or malformed DHCP traffic. Additionally, information on hosts which have successfully completed a DHCP transaction is saved in a database of bindings which may then be used by other security or accounting features.

The screenshot shows the DHCP Snooping configuration page. The global setting is currently set to 'Disabled'. The table below lists 10 ports, all of which are currently set to 'Untrusted'.

Port	Trusted
GigabitEthernet 1/1	Untrusted
GigabitEthernet 1/2	Untrusted
GigabitEthernet 1/3	Untrusted
GigabitEthernet 1/4	Untrusted
GigabitEthernet 1/5	Untrusted
GigabitEthernet 1/6	Untrusted
GigabitEthernet 1/7	Untrusted
GigabitEthernet 1/8	Untrusted
10GigabitEthernet 1/1	Untrusted
10GigabitEthernet 1/2	Untrusted

Parameter descriptions:

Enabled: At the dropdown select Enabled to globally enable DHCP snooping. The default is Disabled.

Port: A row displays for each configurable port.

Trusted: At the dropdown select *Trusted* or *Untrusted* for each port. The default is *Untrusted*.

Buttons:

Cancel: Click to cancel webpage settings.

Apply: Click to save webpage settings to running-config.

System > BLE

This page lets you set BLE (Bluetooth Low Energy) parameters.

This page provides BLE information for wireless CLI access via the MobileApp. (The switch also has a dedicated RJ-45 port for traditional CLI access.) The integrated BLE Radio allows remote access to the switch for troubleshooting and changing settings, reducing time and effort related to console cables and ladders or scissor lifts. Bluetooth Low Energy (BLE) allows remote access to alarm information or to read or change equipment settings without requiring physical access.

Parameter descriptions:

Firmware Version: Displays the current version of BLE (e.g., *LN BLE 1.0.4* or *Not Available*)

BLE MAC Address: Displays the current MAC address of the BLE device. Similar to MAC address for LAN connected devices, Bluetooth devices have an identity address for each device. A Bluetooth address is a 48-bit value that uniquely identifies a Bluetooth device. It is also referred to as a Bluetooth MAC address.

Broadcast: At the dropdown select *Enabled* or *Disabled* for BLE broadcast. The default is *Disabled*.

Connection State: Displays the current BLE Connection state (*BLE Connected* or *BLE Disconnected*).

Buttons:

Disconnect: With BLE in Connected state, click the button to Disconnect from BLE.

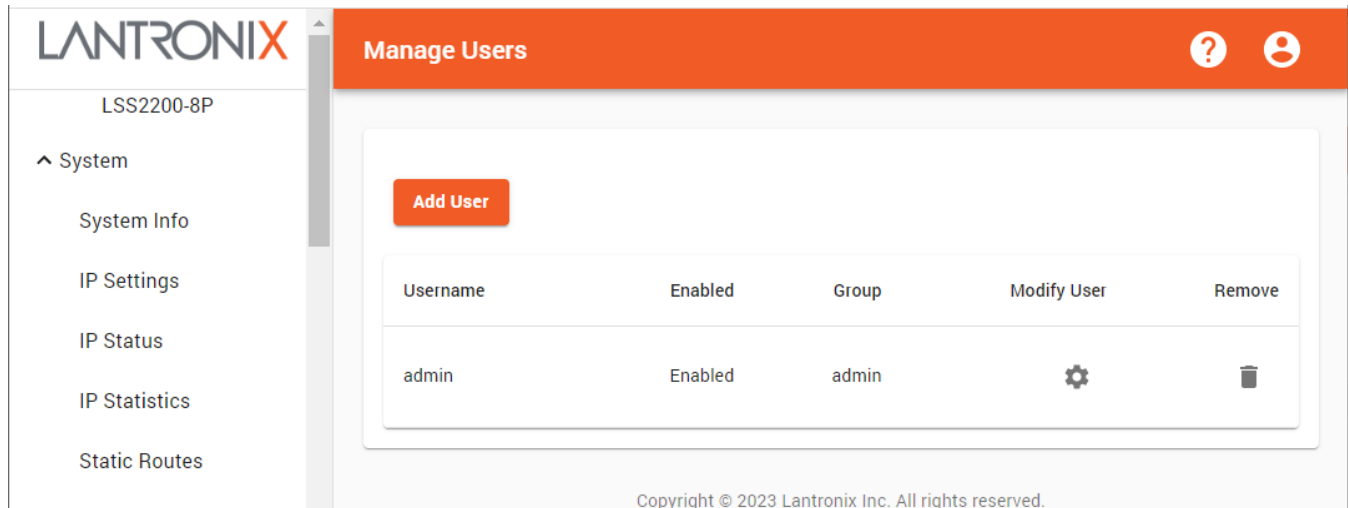
Apply: Click to save webpage settings to running-config.

Messages:

400 Error: Invalid input – DHCP Server undefined already exists

System > Manage Users

This page lets you add, modify, and delete switch users. By default, one user (named admin) is enabled:



Username	Enabled	Group	Modify User	Remove
admin	Enabled	admin		

Parameter descriptions:

Username: Displays a row for each user name.

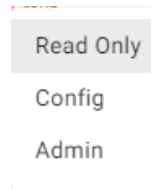
Enabled: Displays the user's current status (e.g., *Enabled* or *Disabled*).

Group: Displays the user's assigned group (*read only*, *admin*, or *config*):

Read Only: This user can view (read) information but cannot configure (write) new or edit existing parameters. A Read Only user can only use show commands to view data and cannot perform config commands.

Config: This user can perform show commands to view data and perform config commands to set parameters.

Admin: This user has full access to any and all CLI commands.



Modify User: Click the icon to display the Modify User page (see below).

Remove: Click the icon in the Remove column of a row to delete the instance.


Add a New User


Click the Add User button to display the Add User dialog. **Note:** only users in the Admin group are allowed to add, modify and delete user accounts. If the current user is not in the Admin group and tries to add, modify or delete a user, the web session is immediately closed, and no user account request is sent to the switch.

Parameter descriptions:

New Username: Enter the new user's username.

Password: Enter the new user's password. Follow your organization's policy for password strength.

 : View the password characters as you type them.

 : Hide the password characters as you type them.

Confirm Password: Enter the new user's password again. It must match the previous Password entry.

Enabled: At the dropdown select *Enabled* to enable the new user.

Group: At the dropdown select the group that this new user should belong to:

Read Only: This user can view (read) information but cannot configure (write) new or edit existing parameters. A Read Only user can only use show commands to view data; cannot perform config commands.

Config: This user can perform show commands to view data and perform config commands to set parameters.

Admin: This user has full access to any and all CLI commands.

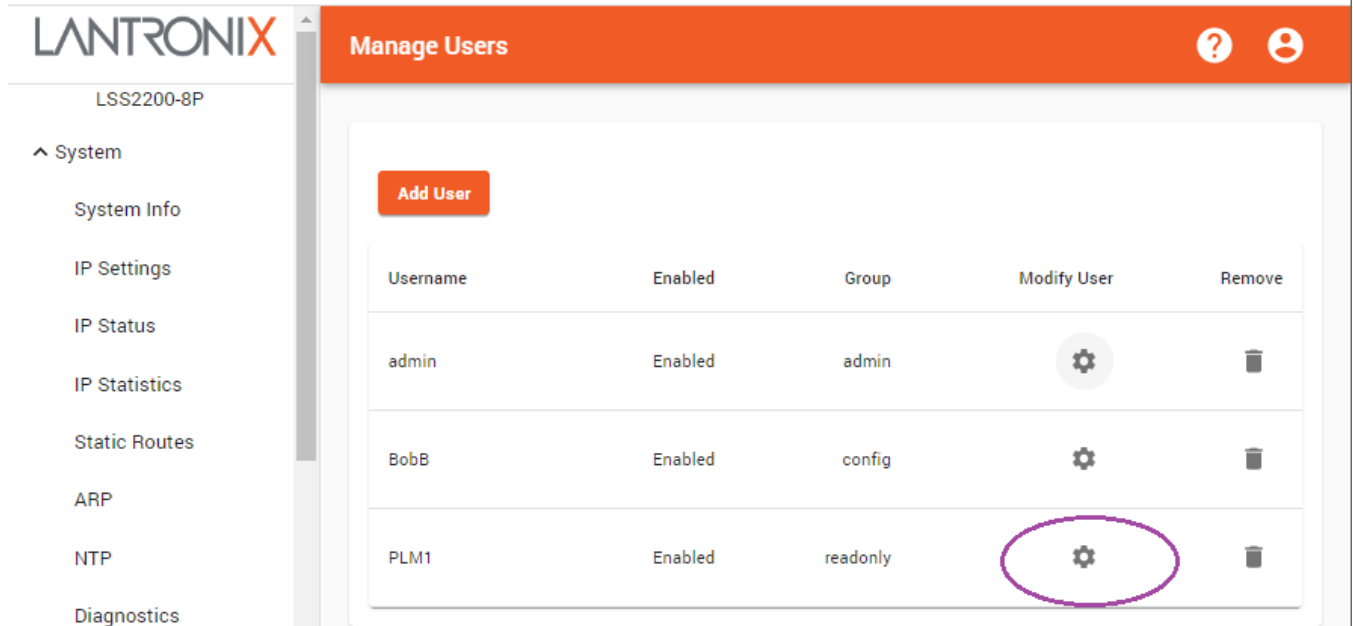
Buttons:

Back: Click to return to the Add User page without saving changes to this page.

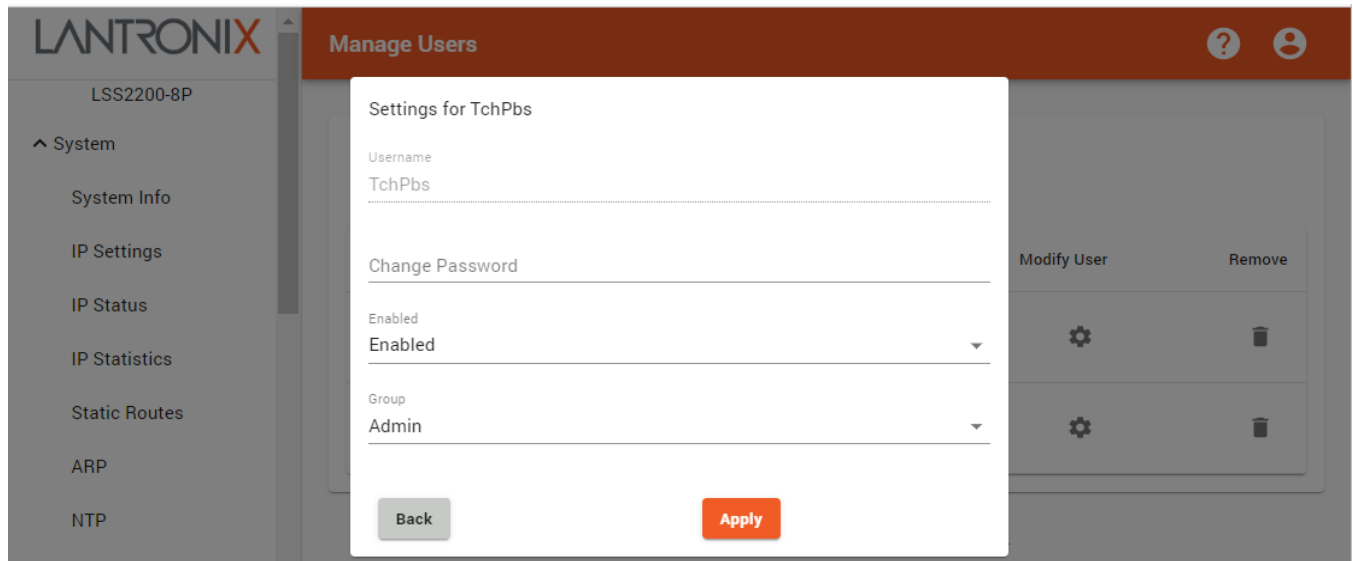
Add User: Click to add the new user to the system.

Modify an Existing User

1. At the Manage Users page click the Modify icon () of the user to modify:



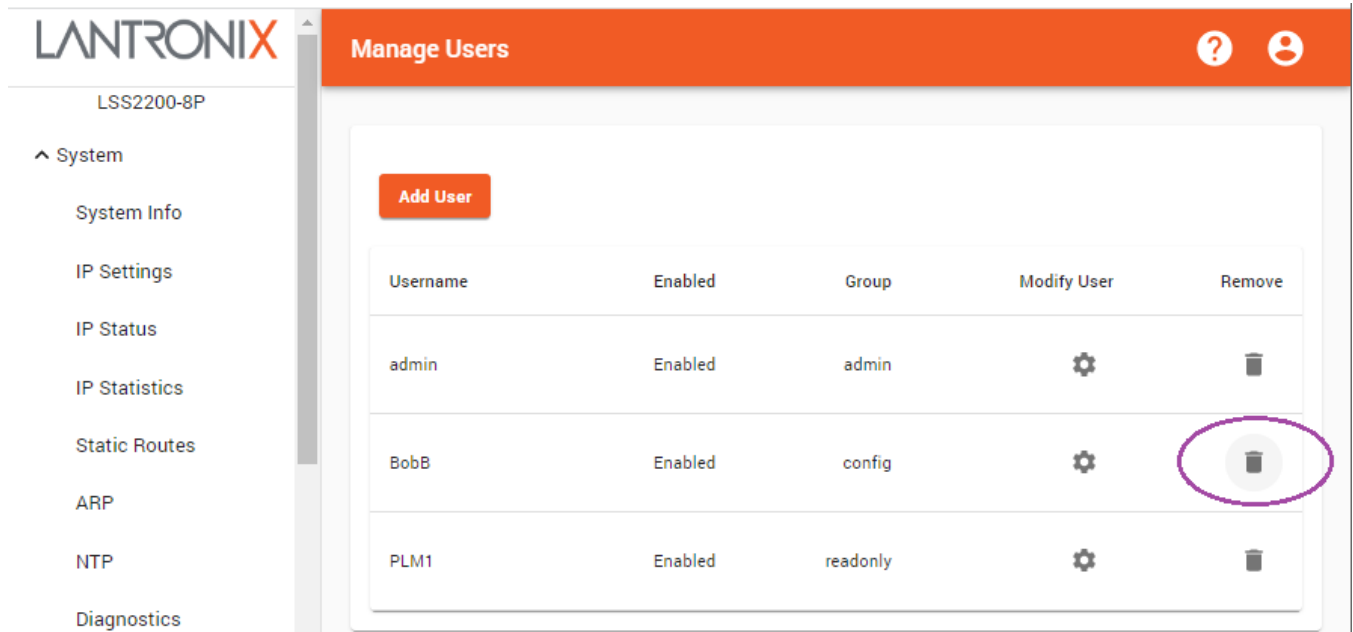
2. At the Settings page, change the selected User's parameters as desired (Username, Password, Enabled, and Group).



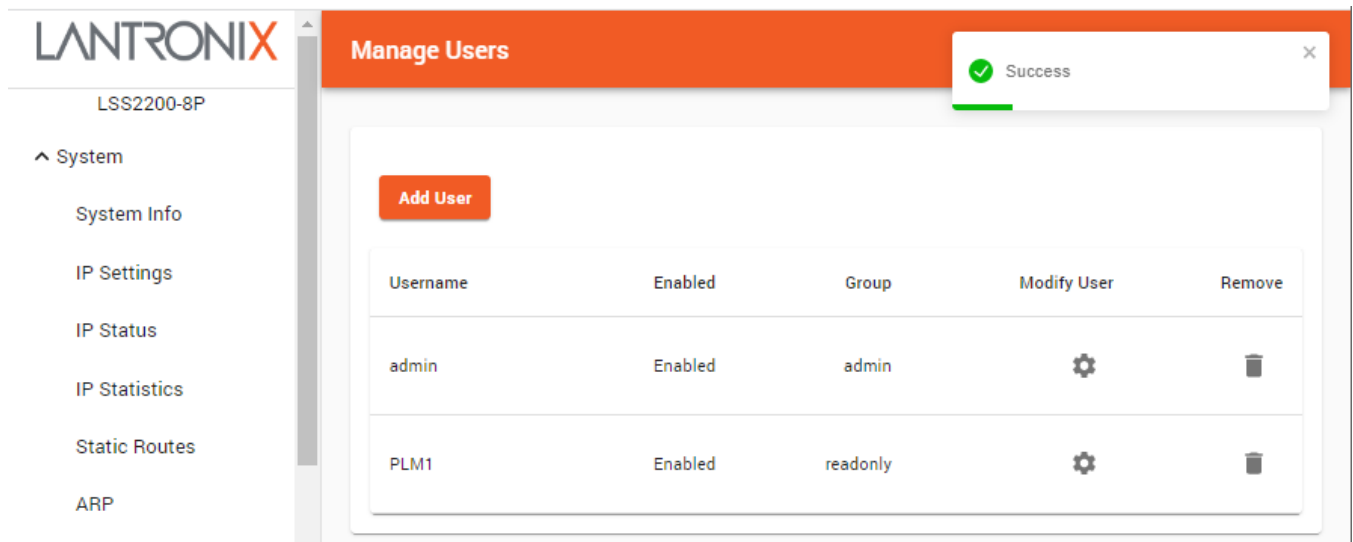
3. Click the Apply button when done.
4. Click the Back button to go back to the Manage Users page and verify the changes.

Remove a User

1. At the Manage Users page click the Remove icon () of the user to modify:



2. At the Manage Users page, verify that the selected user was successfully deleted from the table.



Port Management

This main menu section lets you set and view various port parameters.

Port Management > Port Config

The Port Config page lets you enable and configure GbE and SFP port parameters.

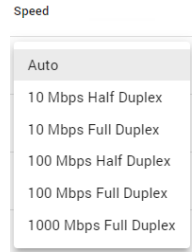
Parameter descriptions:

Port Name: The name of the port. Displays *GigabitEthernet 1/1-1/8* for GbE (copper) ports and *10GigabitEthernet 1/1-1/2* for SFP ports.

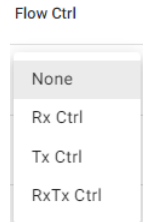
Admin State: At the dropdown select *Enabled* or *Disabled* for each port. The default is *Enabled*.

Description: Entry field for optional description of each port.

Speed: At the dropdown select the desired speed for each port. The options are *10 Mbps Full Duplex*, *100 Mbps Half Duplex*, *100 Mbps Full Duplex*, *100 Mbps Full Duplex*, *1000 Mbps Full Duplex*, and *Auto*. The default is *Auto* (Auto-negotiation).



Flow Ctrl: At the dropdown select the desired flow control setting for each port. The options are *None* (default), *Rx Ctrl*, *Tx Ctrl*, and *RX Tx Ctrl*. (*None* indicates no flow control, *Rx Ctrl* indicates Receive flow control, *Tx Ctrl* indicates Transmit flow control, and *RX Tx Ctrl* indicates Receive and Transmit flow control.)



Jumbo Frame: At the dropdown select Enabled or Disabled for jumbo frames support on copper ports. The max frame size is 10k bytes.

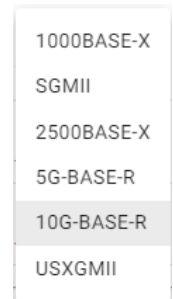
SFP Ports:

Port Name: Displays 10GigabitEthernet 1/1-1/2 for SFP ports.

Admin State: At the dropdown select *Enabled* or *Disabled* for each port. All ports are *Enabled* by default.

Description: Entry field for optional description of each port.

SFP Mode: At the dropdown select one of these SFP port operating modes:



1000BASE-X: Use Gigabit Ethernet (GbE) mode for transmission over fiber. Standards that apply include 1000BASE-LX, 1000BASE-SX, 1000BASE-BX10 1000BASE-LX10, and also the non-standard -ZX and -EX.

SGMII: Use Serial Gigabit Media-Independent Interface mode. SGMII is a variant of MII used for Gigabit Ethernet, but it can also carry 10/100 Mbps Ethernet.

2500BASE-X: Use 2.5Gbps SFP mode in a 2.5Gbps Ethernet network over optical fiber for telecom, enterprise, and other high-performance requirements.

5G-BASE-R: Use 5 Gigabit Ethernet mode over optical fiber.

10G-BASE-R: Use 10 Gigabit Ethernet mode over full-duplex point-to-point links (default). Shared-medium CSMA/CD operation was not carried over from previous Ethernet standards, so half-duplex operation does not exist in 10GbE environments. Default setting.

USXGMII: Use Universal Serial 10GE Media Independent Interface mode for Multi-Gigabit operation at 10M/100M/1G/2.5G/5G/10G bps. USXGMII mode is only used when P #9 and/or P #10 are set to the expansion port and the 2x10GBase-T expansion card ([future release](#)) is installed. If detected, this mode will be selected automatically by the software. When using the TN-SFP-10G-T, the port mode should be set to 10GBase-R.

Flow Ctrl: At the dropdown select the desired flow control setting for each port. The options are:

Flow Ctrl

- None:** indicates no flow control (default setting).
- Rx Ctrl:** indicates Receive flow control,
- Tx Ctrl:** indicates Transmit flow control,
- RX Tx Ctrl:** indicates Receive and Transmit flow control.



Jumbo Frame: At the dropdown select Enabled or Disabled for jumbo frames support on SFP (fiber) ports. The max frame size is 10k bytes. The default setting is *None*.

Buttons:

Apply: Click to save webpage settings to running-config.

Port Management > Port Status

The Port Status page displays the port status parameters set at the Port Management > Port Config webpage.

Port Name	Admin State	Link	Speed	Duplex	Flow Ctrl	Auto	Jumbo Frame
GigabitEthernet 1/1	Enabled	Up	10 Mbps	full	None	Enabled	Disabled
GigabitEthernet 1/2	Enabled	Up	1 Gbps	full	None	Enabled	Disabled
GigabitEthernet 1/3	Enabled	Up	1 Gbps	full	None	Enabled	Disabled
GigabitEthernet 1/4	Enabled	Up	100 Mbps	full	None	Enabled	Disabled
GigabitEthernet 1/5	Enabled	Up	100 Mbps	full	None	Enabled	Disabled
GigabitEthernet 1/6	Enabled	Down	N/A	N/A	N/A	Enabled	Disabled
GigabitEthernet 1/7	Enabled	Down	N/A	N/A	N/A	Enabled	Disabled
GigabitEthernet 1/8	Enabled	Down	N/A	N/A	N/A	Enabled	Disabled
10GigabitEthernet 1/1	Enabled	Down	N/A	N/A	N/A	N/A	Disabled
10GigabitEthernet 1/2	Enabled	Down	N/A	N/A	N/A	N/A	Disabled

Copyright © 2022 Lantronix Inc. All rights reserved.

Parameter descriptions:

Port Name: Displays the name of the port: *GigabitEthernet 1/1-1/8* for GbE (copper) ports and *10GigabitEthernet 1/1-1/2* for SFP ports.

Admin State: Displays the administrative state (*Enabled* or *Disabled*) for each port.

Link: Displays the current link state for each port (*Up* or *Down*).

Speed: Displays the selected speed for each port (e.g., *100 Mbps FDX*, *1000 Mbps HDX*, *1000 Mbps FDX*, *Auto*, or *N/A*).

Duplex: Displays the duplex mode setting set by the Speed setting on the Port Config page (*half* indicates Half Duplex and *full* indicates Full Duplex).

Flow Ctrl: Displays the desired flow control setting for each port. The options are *N/A* (Not Applicable), *None* (default), *Rx Ctrl*, *Tx Ctrl*, and *RX Tx Ctrl*. (*None* indicates no flow control, *Rx Ctrl* indicates Receive flow control, *Tx Ctrl* indicates Transmit flow control, and *RX Tx Ctrl* indicates Receive and Transmit flow control.)

Auto: Displays *Enabled* if the port has *Auto* configuration set on the Port Config page. Otherwise displays *Disabled* or *N/A* (Not Applicable).

Jumbo Frame: Displays the current selection (*Enabled* or *Disabled*) for jumbo frames support for all ports. The default is *Disabled*.

Port Management > Port Statistics

The Port Statistics page displays transmit and receive statistics for each switch port.

Port Name		Bytes	Unicast	Broadcast	Multicast	Discards	Errors	Pause
GigabitEthernet 1/1	Rx	7,547,075	5,139	1,604	31,164	0	11,877	0
	Tx	30,100,148	7,615	34,369	35,400	0	0	0
GigabitEthernet 1/2	Rx	0	0	0	0	0	0	0
	Tx	1,642,204	1	2,387	3,056	0	0	0
GigabitEthernet 1/3	Rx	0	0	0	0	0	0	0
	Tx	0	0	0	0	0	0	0
GigabitEthernet 1/4	Rx	2,492,858	0	7,651	14	0	0	0
	Tx	20,689,352	3	26,037	40,841	0	0	0
GigabitEthernet 1/5	Rx	8,570,917	0	18,187	18,050	0	0	0
	Tx	14,611,165	3	15,499	22,805	0	0	0
GigabitEthernet 1/6	Rx	2,609,678	0	7,541	6	0	0	0
	Tx	20,572,404	3	26,145	40,849	0	0	0
GigabitEthernet 1/7	Rx	8,335,804	0	30	17,337	0	0	0

Parameter descriptions:

Port Name: The table displays a line for each port (e.g., *GigabitEthernet 1/1*).

Bytes: The number of bytes Rx (received) and Tx (transmitted) on the interface, including framing characters.

Unicast: The number of unicast packets received from and delivered to a higher-layer protocol.

Broadcast: The number of broadcast packets received from and delivered to a higher-layer protocol.

Multicast: The number of multicast packets received from and delivered to a higher-layer protocol.

Discards: The number of Rx (inbound) and Tx (outbound) packets that are discarded even if the packets are normal.

Errors: The number of Rx (inbound) and Tx (outbound) packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Pause: The number of Rx (inbound) and Tx (outbound) pause packets.

Buttons:

Clear: Click to clear the webpage data.

Auto-refresh: Automatically refresh the webpage every 3 seconds.

Port Management > PVLAN Config

This page lets you configure Private VLANs. PVLANS allow ports to form a private network. A port must be a member of a PVLAN to forward/receive frames to/from other ports in that PVLAN.

The screenshot shows the Lantronix PVLAN Config web interface. The main content area displays a table with the following data:

Port	PVLANS
GigabitEthernet 1/1	1
GigabitEthernet 1/2	1,10
GigabitEthernet 1/3	1,2,8
GigabitEthernet 1/4	1
GigabitEthernet 1/5	1,2
GigabitEthernet 1/6	1
GigabitEthernet 1/7	1
GigabitEthernet 1/8	1
10GigabitEthernet 1/1	1
10GigabitEthernet 1/2	1

At the top right of the interface, a green success message is displayed: "Success". At the bottom right, there are "Cancel" and "Apply" buttons. The footer of the interface reads: "Copyright © 2023 Lantronix Inc. All rights reserved."

Parameter descriptions:

Port: The table displays a line for each port (e.g., *GigabitEthernet 1/1* or *10GigabitEthernet 1/2*).

PVLANS: Enter the Private VLAN ID for one or more private VLANs. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears.

Buttons:

Cancel: Click to ignore webpage settings.

Apply: Click to save webpage settings to running-config.

Messages:

400 Error: Port should be part of at least one PVLAN : 10

Port Management > Port VLAN Config

This page lets you configure port VLANs. Port-based VLANs group VLAN members by port. A port forwards traffic for a VLAN only after it is assigned to the VLAN.

Port Name	Mode	Port VLAN	Allowed VLANs
GigabitEthernet 1/1	Access	1	
GigabitEthernet 1/2	Access	4	
GigabitEthernet 1/3	Trunk	2	1,10
GigabitEthernet 1/4	Trunk	3	1,2,11-15
GigabitEthernet 1/5	Access	1	
GigabitEthernet 1/6	Access	1	
GigabitEthernet 1/7	Access	1	
GigabitEthernet 1/8	Access	1	
10GigabitEthernet 1/1	Access	1	
10GigabitEthernet 1/2	Access	1	

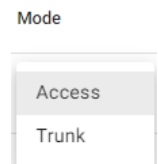
Parameter descriptions:

Port Name: The table displays a line for each port (e.g., *GigabitEthernet 1/1*).

Mode: At the dropdown select an operating mode for each port:

Access: An Access port belongs to only one VLAN and sends traffic untagged. Access ports are usually used to connect a terminal device unable to identify VLAN-tagged packets or are used when separating different VLAN members is unnecessary. Access mode is the default VLAN Mode setting.

Trunk: A Trunk port carries multiple VLANs to receive and send traffic for them. Except for traffic from the port VLAN ID (PVID), traffic sent through a Trunk port will be VLAN-tagged. Ports that connect network devices are usually configured as Trunk ports.



Port VLAN: Select a VLAN ID in the range 1-4094. By default, VLAN 1 is the port VLAN ID (PVID) for all ports.

Allowed VLANs: Enter the VLAN IDs that are to be allowed. This can be an individual VLAN ID or a range of VLAN IDs, or a combination of both.

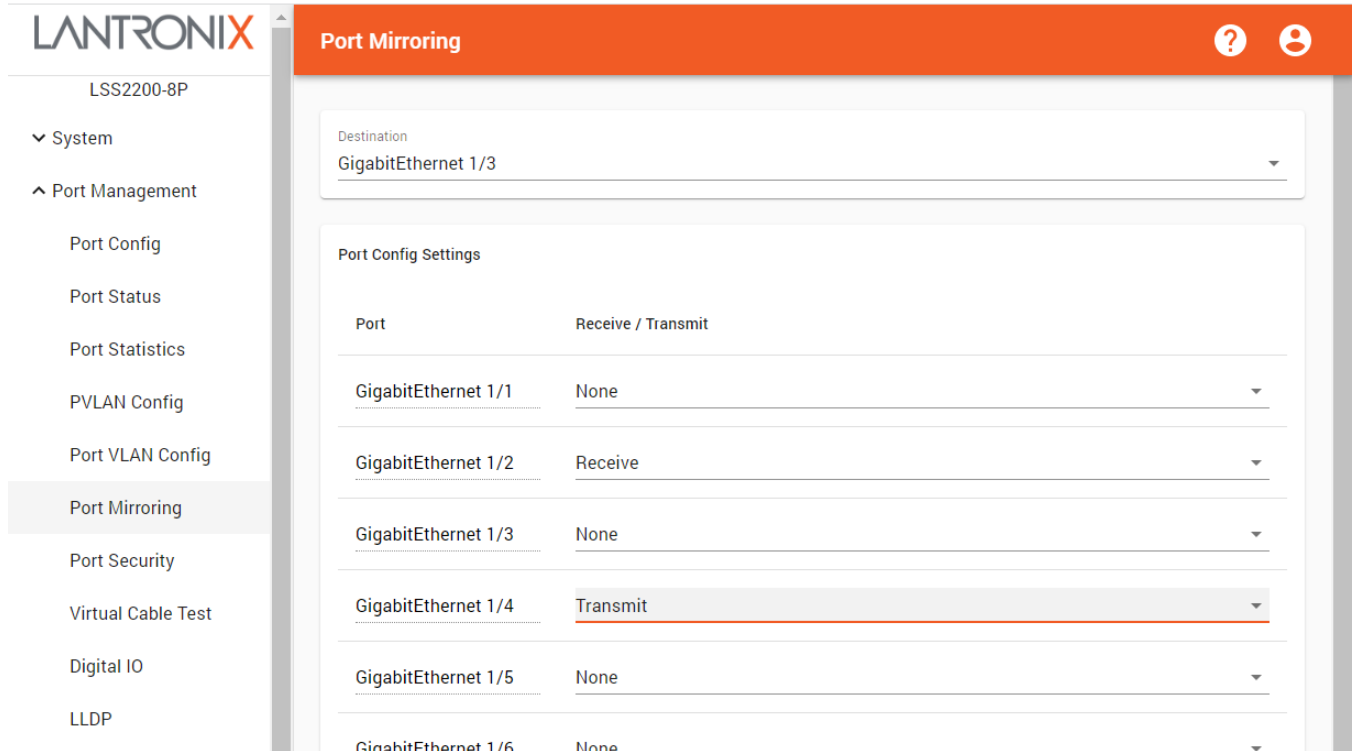
Buttons:

Cancel: Click to ignore webpage settings.

Apply: Click to save webpage settings to running-config.

Port Management > Port Mirroring

Port mirroring can be used on the switch to send a copy of network packets seen on the specified port (source port) to another specified port (destination port). With port mirroring enabled, the packets can be monitored and analyzed.



Parameter descriptions:

Destination: At the dropdown select the desired port (e.g., *GigabitEthernet 1/1* or *10GigabitEthernet 1/2*).

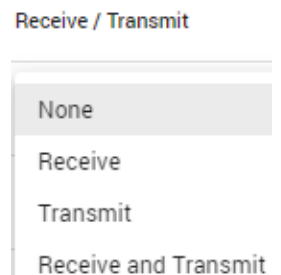
Port: The table displays a line for each port (e.g., *GigabitEthernet 1/1*).

Receive / Transmit: At the dropdown select the desired mirror mode (*None*, *Receive*, *Transmit*, or *Receive and Transmit*). The default is *None*.

Buttons:

Cancel: Click to ignore any webpage changes.

Apply: Click to save webpage settings to running-config.



Message: 404 Error: Global port mirror settings are not configured

Port Management > Port Security

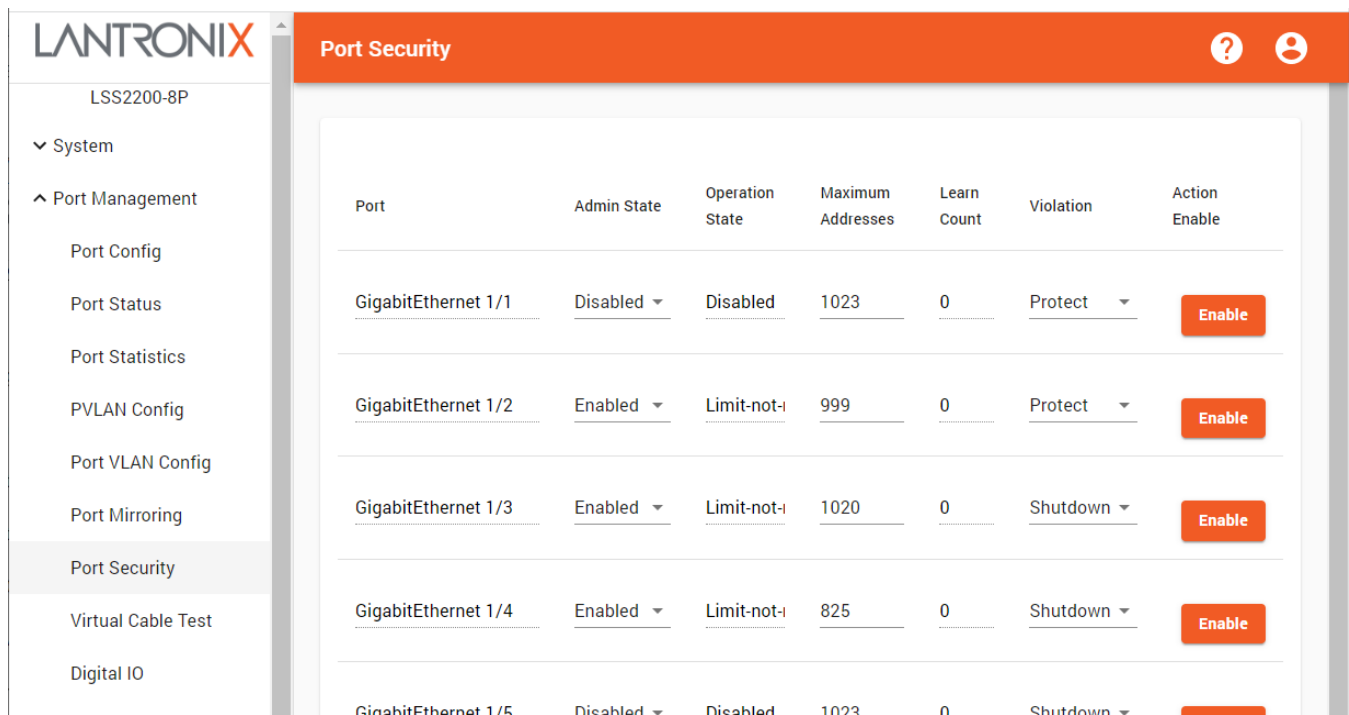
The port security feature lets you restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port.

Port Security with Dynamically Learned and Static MAC Addresses

You can use port security with dynamically-learned and static MAC addresses to restrict any port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into that port. When you assign secure MAC addresses to a secure port, the port does not forward ingress traffic having source addresses not within the group of defined addresses. Limiting the number of secure MAC addresses to one and assigning just one secure MAC address, the device attached to that port gets the full bandwidth of the port.

A security violation occurs in either of these situations:

- When the maximum number of secure MAC addresses is reached on a secure port, and the source MAC address of the ingress traffic is different than any of the identified secure MAC addresses, port security applies the configured 'Violation' mode.
- If traffic with a secure MAC address that is configured or learned on one secure port attempts to access another secure port in the same VLAN, applies the configured Violation mode.



Port	Admin State	Operation State	Maximum Addresses	Learn Count	Violation	Action Enable
GigabitEthernet 1/1	Disabled	Disabled	1023	0	Protect	Enable
GigabitEthernet 1/2	Enabled	Limit-not-reached	999	0	Protect	Enable
GigabitEthernet 1/3	Enabled	Limit-not-reached	1020	0	Shutdown	Enable
GigabitEthernet 1/4	Enabled	Limit-not-reached	825	0	Shutdown	Enable
GigabitEthernet 1/5	Disabled	Disabled	1023	0	Shutdown	Enable

Parameter descriptions:

Port: The table displays a line for each port (e.g., *GigabitEthernet 1/1*).

Admin State: At the dropdown select the Port Security administrative state (*Enabled* or *Disabled*). The default is *Disabled*.

Operation State: Displays the Port Security operational state (e.g., *Enabled*, *Disabled*, *limit-not-reached*).

Maximum Addresses: Enter the highest number of MAC addresses to be configured for Port Security. The valid range is 1-1023.

Learn Count: Displays the number of learned addresses from inbound traffic from the connected device.

Violation: At the dropdown select the response to take for a violation (*Protect* or *Shutdown*). A security violation occurs if the maximum number of secure MAC addresses has been added to the address table and the port receives traffic from a MAC address that is not in the address table. You can configure the port for one of these violation modes:

Protect: Drops packets with unknown source MAC addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value. The default is *Protect*.

Shutdown: Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

Violation

Protect

Shutdown

Action Enable: Click the button to enable the settings for the row (port).

Buttons:

Cancel: Click to cancel webpage settings.

Apply: Click to save webpage settings to running-config.

Messages:

400 Error: Input payload validation failed
AGING_TIME: 1e+37 is greater than maximum of 956

400 Error: Input payload validation failed
AGING_TIME: 0 is less than the minimum of 4

400 Error: Input payload validation failed
MAXIMUM: 999999999999 is greater than the maximum of 1023.

Port Management > Virtual Cable Test

The Virtual Cable Tester uses TDR (Time Domain Reflectometry) for remote identification of potential cable malfunctions. It detects and reports potential cabling issues such as pair swaps, pair polarity, and excessive skew. It can also detect cable opens, shorts, or impedance mismatch in the cable and report accurately within one meter the distance to the fault.

Note:

- Do not change the port configuration while the test is running.
- Do not run the Virtual Cable Test on the Management port during active traffic.
- Do not change port status (e.g., remove the cable at the near or far end) as the results may be inaccurate.
- **WARNING:** Running cable test will temporarily bring down the affected link.

LANTRONIX
Virtual Cable Test
? ⚙

LSS2200-8P

- ▼ System
- ▼ Port Management
- ▼ PoE Management
- ▼ SNMP
- ▼ Notifications
- ▼ Maintenance

ConsoleFlow

Lantronix Provision Manager

WARNING: Running cable test will temporarily bring down the affected link.

Test	Port	Timestamp	Pair A		Pair B		Pair C		Pair D	
			Status	Length	Status	Length	Status	Length	Status	Length
<input type="checkbox"/>	GigabitEthernet 1/1	2023-02-01 12:02:54	Pair Open	0 m	Pair Open	0 m	Pair Ok	- m	Pair Ok	- m
<input type="checkbox"/>	GigabitEthernet 1/2	2023-02-01 12:08:45	Pair Open	2 m	Pair Open	1 m	Pair Open	2 m	Pair Open	2 m
<input type="checkbox"/>	GigabitEthernet 1/3	2023-02-01 12:09:15	Pair Open	0 m	Pair Open	0 m	Pair Open	0 m	Pair Open	1 m
<input type="checkbox"/>	GigabitEthernet 1/4	2023-02-01 12:09:27	Pair Open	0 m	Pair Open	0 m	Pair Short	1 m	Pair Short	1 m
<input type="checkbox"/>	GigabitEthernet 1/5	2023-02-01 12:09:36	Pair Ok	- m	Pair Ok	- m	Pair Open	0 m	Pair Open	0 m
<input type="checkbox"/>	GigabitEthernet 1/6	2023-02-01 12:09:48	Pair Open	0 m	Pair Open	0 m	Pair Open	1 m	Pair Short	1 m
<input type="checkbox"/>	GigabitEthernet 1/7	2023-02-01 12:10:03	Pair Open	0 m	Pair Open	1 m	Pair Short	0 m	Pair Short	0 m
<input type="checkbox"/>	GigabitEthernet 1/8	2023-02-01 12:10:06	Pair Open	2 m	Pair Open	3 m	Pair Open	2 m	Pair Open	3 m

Cancel
Apply

Copyright © 2023 Lantronix Inc. All rights reserved.

Parameter descriptions:

Test: Check the box to enable a virtual cable test on the port.

Port: The table displays a line for each port (e.g., *GigabitEthernet 1/1*).

Timestamp: The date and time that the test was run.

Pair A, B, C, D: Each cable pair has a column for Status and Length.

Status: The status of the cable pair:

Unknown: none of the following.

Pair Ok: The cable test showed no issues.

Normal: the pair is properly terminated at the remote end. 'Distance To Fault' is a blank.

Pair Open: the pair is open.

Pair Short: the pair is shorted.

ImpedanceMismatch: the impedance of the pair is mismatched.

Not Tested: displays if the test has not yet been run.


Length: The distance to the fault point of the cable pair (the overall distance to the fault in Meters). A blank field indicates 'Status' is 'normal' or this value is invalid.

Buttons:

Cancel: Click to cancel webpage settings.

Apply: Click to save webpage settings to running-config.

Messages:

Message:  and 

Meaning: When using the management port, sometimes an Error status is displayed and the webpage fails to refresh. This might be due to the webpage refresh being initiated while the management port is down from the network outage.

Recovery: Manually refresh the webpage.

Port Management > Digital IO

This page lets you set and view Digital I/O (DIO) parameters. See the Install Guide for related DIO hardware information.

The screenshot shows the 'Digital IO' configuration page in the Lantronix web interface. The page is titled 'Digital IO' and features a sidebar on the left with navigation options. The main content area is divided into two sections: 'Digital IO Config' and 'Digital IO Status'. The 'Digital IO Config' section contains a table with columns for Digital IO Port Number, Port Name, Direction, Active State, SNMP Trap Enabled, and Trap Trigger. The 'Digital IO Status' section contains a table with columns for Digital IO Port Number, Direction, and Status. At the bottom right, there are 'Cancel' and 'Apply' buttons.

Parameter descriptions:

Digital IO Config:

Digital IO Port Number: Displays the digital I/O port number (instance) (1 or 2).

Port Name: At the dropdown select the port to be used for each row (e.g., *GigabitEthernet 1/2*).

Direction: At the dropdown select the direction to be used for each row (*Input* or *Output*). The default is *Input*. Input is typically related to switches, potentiometers, sensors, cameras, etc. Output is typically related to electric motors, lighting devices, alarms, etc.

Active State: At the dropdown select the mode for the DIO active state for each row (*Normally closed*, *Normally open*, or *Off*). The default is *Off*.

SNMP Trap Enabled: At the dropdown select whether SNMP traps are *Enabled* or *Disabled*. The default is *Disabled*.

Trap Trigger: At the dropdown select how the SNMP trap is to be triggered (*Low to High*, *High to Low*, or *None*). The default is *Low to High*.

Digital IO Status:

Digital IO Port Number: Displays the digital I/O port number (instance) (1 or 2).

Direction: Displays the direction that is set for each row (*Input* or *Output*).

Status: Displays the current I/O state (*Low* or *High*).

Direction

Input
Output

Active State

Normally closed
Normally open
Off

Trap Trigger

Low to High
High to Low

Buttons:

Cancel: Click to cancel webpage settings.

Apply: Click to save webpage settings to running-config.

Example:

The screenshot displays the Digital IO configuration interface for the LSS2200-8P switch. The interface is divided into two main sections: 'Digital IO Config' and 'Digital IO Status'. A 'Success' message is visible in the top right corner.

Digital IO Port Number	Port Name	Direction	Active State	STAMP Trap Enabled	Trap Trigger
1	GigabitEthernet1/2	Output	Normally closed	Disabled	Low to High
2	10GigabitEthernet1/2	Input	Normally open	Enabled	Low to High

Digital IO Port Number	Direction	Status
1	output	Low
2	input	Low

Message: 404 Error: Digital I/O configuration data not found.

Problem: Digital IO Config and Status break after upgrade from v1.5.0.0R16 to v1.6.0.0R6.

Description: After upgrading from v1.5.0.0R16 to v1.6.0.0R6, the Digital IO webpages stop displaying, and the CLI commands don't return anything.

Recovery: To restore Digital IO functionality:

1. Backup the running config to a remote file.
2. Edit the backup file to remove all "DIO*" commands.
3. Restore running-config from the edited backup file.
4. If the restore succeeds, then optionally change Digital IO settings as desired, and then copy running-config to startup-config.

If the above steps fail, try these steps (note that the following procedure would lose all modified config settings):

1. Reload Factory Defaults.
2. Copy the running-config to the startup-config.
3. Reboot the switch.

Message: 400 Error: Input payload validation failed

PORT_NUM: "1" is not of 'integer'

ACTIVE_STATE: " is not one of ['high', 'low', 'None']

Description: An invalid DIO parameter was entered.

Recovery: 1. Click the OK button to clear the message. 2. Enter valid DIO parameter(s). 3. Click the Apply button.

Port Management > LLDP

The LLDP page lets you set and view LLDP and LLDP-MED parameters.

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol used by network devices for advertising their identity, capabilities, and neighbors on a local area network based on IEEE 802 technology, principally wired Ethernet. LLDP is used in network management and network monitoring applications, and to advertise PoE capabilities and requirements and negotiate power delivery.

LLDP-MED (Media Endpoint Discovery) is an enhancement of LLDP that provides these facilities:

- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority, and Diffserv) settings enabling plug and play networking.
- Device location discovery to allow creation of location databases and, for VoIP, Enhanced 911 services.
- Extended and automated power management of Power over Ethernet (PoE) end points.
- Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, serial or asset number).

LLDP information is sent by devices from each of their interfaces at a fixed interval, in the form of an Ethernet frame. Each frame contains one LLDP Protocol Data Unit (PDU). Each LLDP PDU is a sequence of type-length-value (TLV) structures. The Ethernet frame used in LLDP typically has its destination MAC address set to a special multicast address that 802.1D-compliant bridges do not forward. Other multicast and unicast destination addresses are permitted. The EtherType field is set to 0x88cc. Each LLDP frame starts with these mandatory TLVs: Chassis ID, Port ID, and Time-to-Live. The mandatory TLVs can be followed by a number of optional TLVs.

The screenshot shows the LLDP configuration page for the LSS2200-8P device. The sidebar on the left contains navigation options such as System, Port Management, PoE Management, and SNMP. The main content area is titled 'LLDP Configuration' and includes a table for configuring LLDP parameters across various ports.

LLDP Configuration			
Tx Interval	Holdtime		
30	s 4		
Port	Rx Enable All <input type="checkbox"/>	Tx Enable All <input type="checkbox"/>	MED Enable All <input type="checkbox"/>
GigabitEthernet 1/1	Disabled	Disabled	Disabled
GigabitEthernet 1/2	Disabled	Disabled	Disabled
GigabitEthernet 1/3	Disabled	Disabled	Disabled
GigabitEthernet 1/4	Disabled	Disabled	Disabled
GigabitEthernet 1/5	Disabled	Disabled	Disabled
GigabitEthernet 1/6	Disabled	Disabled	Disabled
GigabitEthernet 1/7	Disabled	Disabled	Disabled
GigabitEthernet 1/8	Disabled	Disabled	Disabled
10GigabitEthernet 1/1	Disabled	Disabled	Disabled
10GigabitEthernet 1/2	Disabled	Disabled	Disabled

Parameter descriptions:

LLDP Configuration:

Tx Interval: Enter an LLDP transmit interval time in seconds. The valid range is 5-32768 seconds. The default is 30 seconds.

Holdtime: Enter an LLDP hold time in seconds. 2-10 seconds. The default is 4 seconds.

PORT: The table displays a line for each port (e.g., *GigabitEthernet 1/1*).

Rx | Enable All Tx | Disable All MED | Disable All

Rx | Enable All: Check the checkbox to enable all LLDP receive direction transmissions. Uncheck the box to disable all LLDP receive direction transmissions.

Tx | Enable All: Check the checkbox to enable all LLDP transmit direction transmissions. Uncheck the box to disable all LLDP transmit direction transmissions.

MED | Enable All: Check the checkbox to enable all LLDP-MED Tx and Rx.

The screenshot displays the LLDP configuration page for the LSS2200-8P device. At the top, there are three control boxes: 'Rx | Enable All' (unchecked), 'Tx | Disable All' (checked), and 'MED | Disable All' (checked). A 'Success' notification is visible in the top right. The main configuration area is divided into several sections:

- LLDP Port Settings:** A table showing two ports, both with 'Enabled' status for Tx and Rx.
- LLDP MED:** A table with columns for Port, MED Cap, Device Type, SW Revision, HW Revision, Manufacturer, Model, Network Policy, Power Type, Power Requested, and Power Allocate. The entry for GigabitEthernet 1/1 shows 'LLDP-MED Capabilities' and 'Endpoint Class 1'.
- LLDP Neighbors:** A table with columns for Port, Chassis ID, Port ID, Port Description, System Name, System Description, Management IP, TTL, Time Remaining, and System Capabilities. One neighbor is listed for GigabitEthernet 1/1.
- LLDP Statistics:** A summary table showing Tx (1), RxInvalid (0), RxValid (4), and Expired (0).

LLDP MED:

Port: The table displays a line for each port (e.g., *GigabitEthernet 1/1*).

MED Cap: Displays the set of LLDP-MED capabilities (e.g., *LLDP-MED Capabilities, NP, LI, PS*). The LLDP MED Codes are (NP) Network Policy, (LI) Location Identification, (PS) Power Source Entity, (PD) Power Device, and (IN) Inventory.

Device Type: Displays the type of LLDP-MED device. Any LLDP-MED Device operates as a specific type of LLDP-MED Device, which may be either a Network Connectivity Device or a specific Class of Endpoint Device.

A Network Connectivity Device is a LLDP-MED Device that provides access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of these technologies: **1.** LAN Switch/Router, **2.** IEEE 802.1 Bridge, **3.** IEEE 802.3 Repeater, **4.** IEEE 802.11 Wireless Access Point, or **5.** Any device that supports the IEEE 802.1AB and MED extensions that can relay IEEE 802 frames via any method.

An Endpoint Device is an LLDP-MED Device that sits at the network edge and provides some aspect of IP communications service, based on IEEE 802 LAN technology.

The main difference between a Network Connectivity Device and an Endpoint Device is that only an Endpoint Device can start the LLDP-MED information exchange. Even though a switch should always be a Network Connectivity Device, it is possible to configure it to act as an Endpoint Device, and thereby start the LLDP-MED information exchange (in the case where two Network Connectivity Devices are connected together).

SW Revision: Displays the neighbor device's software rev (e.g., *v1.2.3* or *not advertised*).

HW Revision: Displays the neighbor device's hardware rev (e.g., *v1.0.3* or *not advertised*).

Manufacturer: Displays name of the maker of the neighbor device.

Model: Displays the model number or name of the neighbor device if advertised.

Network Policy: Displays the neighbor device's network policy if advertised.

Power Type: Displays the neighbor device's power type (e.g., PSE (Power Sourcing Equipment)).

Power Requested: Displays the neighbor device's power requested.

Power Allocated: Displays the amount of power allocated to the neighbor device.

LLDP Neighbors:

Port: The table displays a line for each port (e.g., *GigabitEthernet 1/1*).

Chassis ID: Displays the LLDP neighbor's Chassis identifier (the MAC address for the chassis).

Port ID: Displays the LLDP neighbor's Port identifier (the port number or the MAC address).

Port Description: The identifier for the port.(e.g., *eth0* or *Port #9*).

System Name: Displays the administratively-assigned name for the system (e.g., *SM24TBT2DPB* or *axis-acc8ebaf7c1*).

System Description: Displays the name of the switch if available.

Management IP: Displays the IP address of the LLDP neighbor (e.g., *192.168.1.77*).

TTL: Displays the configured time to live (e.g., *117* seconds).

Time Remaining: Displays the remaining time to live (TTL, e.g., *95* seconds).

System Capabilities: Displays the neighbor device's capabilities (e.g., *Bridge (Switch):On* or *Bridge (Switch):Off, WLAN Access Point:Off, Router:Off, Station:On*).

System
Capabilities

Bridge
(Switch):Off,
WLAN Access
Point:Off,
Router:Off,
Station:On

LLDP Statistics:

Tx: Displays the number of LLDP transmit frames.

RxValid: Displays the number of valid LLDP receive frames.

RxInvalid: Displays the number of invalid LLDP receive frames. Received BPDUs that failed validation checks and were dropped.

Expired: Displays the number of expired LLDP frames.

Buttons:

Clear: Click to clear the webpage data.

Cancel: Click to ignore the webpage changes.

Apply: Click to save webpage settings to running-config.

Messages:

400 Error: Input payload validation failed

TXINTERVAL:0 is less than the minimum of 5

TXHOLDMULTIPLIER: 1 is less than the minimum of 2

400 Error: Input payload validation failed

TXHOLDMULTIPLIER: 11 is greater than the maximum of 10

Port Management > Spanning Tree

The Spanning Tree page lets you set and view Bridge and Port settings and view Port Statistics and Port Status.

The Spanning Tree Protocol (STP) is a network protocol that builds a loop-free logical topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. STP creates a spanning tree that characterizes the relationship of nodes within a network of connected layer-2 bridges and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes.

This page has four sections; Bridge Settings, Port Settings, Port Statistics, and Port Status as shown and described below.

Bridge Settings

Bridge Settings	
Enabled	Disabled
Protocol Version	RSTP
Priority	32768
Forward Delay	15 s
Max Age	20 s
Transmit Hold Count	6
Topology Changes	0
Running	False

Parameter descriptions:

Enabled: Displays *Enabled* if currently running, otherwise *Disabled*. The default is *Disabled*.

Protocol Version: At the dropdown select the protocol to use (*RSTP*).

Priority: Enter or select the desired priority. The valid range is 4096-61440. The default is 32768. It must be a multiple of 4096.

Forward Delay: Enter or select the desired forward delay time in seconds. The valid range is 4-30 seconds. The default is 15 seconds.

Max Age: Enter or select the desired maximum STP aging time in seconds. The valid range is 6-40 seconds. The default is 20 seconds.

Transmit Hold Count: Enter or select the desired TX hold count. The valid range is 1-10 seconds. The default is 6 seconds.

Topology Changes: Displays the number of changes in topology (e.g., 0 or 1).

Running: Displays *true* if STP is currently running, otherwise *false*.

Port Settings:

Port	Auto Path Cost	Auto Path Cost	Priority	Admin Edge	Auto Edge	Point To Point	Restricted Role	Restricted TCN
GigabitEthernet 1/1	Enabled ▾	_____	128	Disabled ▾	Enabled ▾	Auto ▾	Disabled ▾	Disabled ▾
GigabitEthernet 1/2	Enabled ▾	_____	128	Disabled ▾	Enabled ▾	Auto ▾	Disabled ▾	Disabled ▾
GigabitEthernet 1/3	Enabled ▾	_____	128	Disabled ▾	Enabled ▾	Auto ▾	Disabled ▾	Disabled ▾
GigabitEthernet 1/4	Enabled ▾	_____	128	Disabled ▾	Enabled ▾	Auto ▾	Disabled ▾	Disabled ▾
GigabitEthernet 1/5	Enabled ▾	_____	128	Disabled ▾	Enabled ▾	Auto ▾	Disabled ▾	Disabled ▾
GigabitEthernet 1/6	Enabled ▾	_____	128	Disabled ▾	Enabled ▾	Auto ▾	Disabled ▾	Disabled ▾
GigabitEthernet 1/7	Enabled ▾	_____	128	Disabled ▾	Enabled ▾	Auto ▾	Disabled ▾	Disabled ▾
GigabitEthernet 1/8	Enabled ▾	_____	128	Disabled ▾	Enabled ▾	Auto ▾	Disabled ▾	Disabled ▾
10GigabitEthernet 1/1	Enabled ▾	_____	128	Disabled ▾	Enabled ▾	Auto ▾	Disabled ▾	Disabled ▾
10GigabitEthernet 1/2	Enabled ▾	_____	128	Disabled ▾	Enabled ▾	Auto ▾	Disabled ▾	Disabled ▾

Parameter descriptions:

Port: The table displays a line for each port (e.g., *GigabitEthernet 1/1*).

Auto Path Cost: At the dropdown select *Enabled* or *Disabled*. The default is *Enabled*.

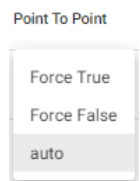
Auto Path Cost: Enter the desired automatic path cost. The valid range is 1-3.

Priority: Enter the desired priority value. This can be used to control priority of ports having identical path cost. The valid range is 16-240 and it must be a multiple of 16. The default is 128.

Admin Edge: At the dropdown select *Enabled* or *Disabled*. The default is *Enabled*. This controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized.)

Auto Edge: At the dropdown select *Enabled* or *Disabled*. The default is *Disabled*. This controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.

Point To Point: At the dropdown select the desired point to point mode (*Force True*, *Force False*, or *auto*). The default is *auto*. This controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.



Restricted Role: At the dropdown select *Enabled* or *Disabled*. The default is *Disabled*. If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it

can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network from influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

Restricted TCN: At the dropdown select *Enabled* or *Disabled*. The default is *Disabled*. If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

Port Statistics:

Port Statistics												
Port	Rx Invalid	Rx Unknown	Rx STP	Rx TCN	Rx RST	Rx MST	Rx SPT	Tx STP	Tx TCN	Tx RST	Tx MST	Tx SPT
GigabitEthernet 1/1	0	0	0	0	0	0	0	0	0	0	0	0
GigabitEthernet 1/2	0	0	0	0	0	0	0	0	0	0	0	0
GigabitEthernet 1/3	0	0	0	0	0	0	0	0	0	0	0	0
GigabitEthernet 1/4	0	0	0	0	0	0	0	0	0	0	0	0
GigabitEthernet 1/5	0	0	0	0	0	0	0	0	0	0	0	0
GigabitEthernet 1/6	0	0	0	0	0	0	0	0	0	0	0	0
GigabitEthernet 1/7	0	0	0	0	0	0	0	0	0	0	0	0
GigabitEthernet 1/8	0	0	0	0	0	0	0	0	0	0	0	0
10GigabitEthernet 1/1	0	0	0	0	0	0	0	0	0	0	0	0
10GigabitEthernet 1/2	0	0	0	0	0	0	0	0	0	0	0	0

Port: The table displays a line for each port (e.g., *GigabitEthernet 1/1*).

Rx Invalid: The number of BPDUs received on the port that are not valid.

Rx Unknown: The number of BPDUs received on the port that are not known.

Rx STP: The number of legacy STP Configuration BPDU's received on the port.

Rx TCN: The number of (legacy) Topology Change Notification BPDU's received on the port.

Rx RST: The number of RSTP Configuration BPDU's received on the port.

Rx MST: The number of MSTP Configuration BPDU's received on the port.

Rx SPT: The number of receive SPTs.

Tx STP: The number of legacy STP Configuration BPDU's received/transmitted on the port.

Tx TCN: The number of (legacy) Topology Change Notification BPDU's transmitted on the port.

Tx RST: The number of RSTP Configuration BPDU's transmitted on the port.

Tx MST: The number of MSTP Configuration BPDU's transmitted on the port.

Tx SPT: The number of transmit SPTs.

Port Status:

Port	State
GigabitEthernet 1/1	Forwarding
GigabitEthernet 1/2	Forwarding
GigabitEthernet 1/3	Forwarding
GigabitEthernet 1/4	Forwarding
GigabitEthernet 1/5	Forwarding
GigabitEthernet 1/6	Forwarding
GigabitEthernet 1/7	Forwarding
GigabitEthernet 1/8	Forwarding
10GigabitEthernet 1/1	Forwarding
10GigabitEthernet 1/2	Forwarding

Port: The table displays a line for each port (e.g., *GigabitEthernet 1/1*).

State: Displays the current STP state (e.g., *forwarding* or *blocking*).

Buttons:

Cancel: Click to ignore webpage settings.

Apply: Click to save webpage settings to running-config.

Messages:

*400 Error: Input payload validation failed
 auto_path_cost: '3' is not of type 'boolean'
 priority: 136 is not a multiple of 16*

Port Management > QoS

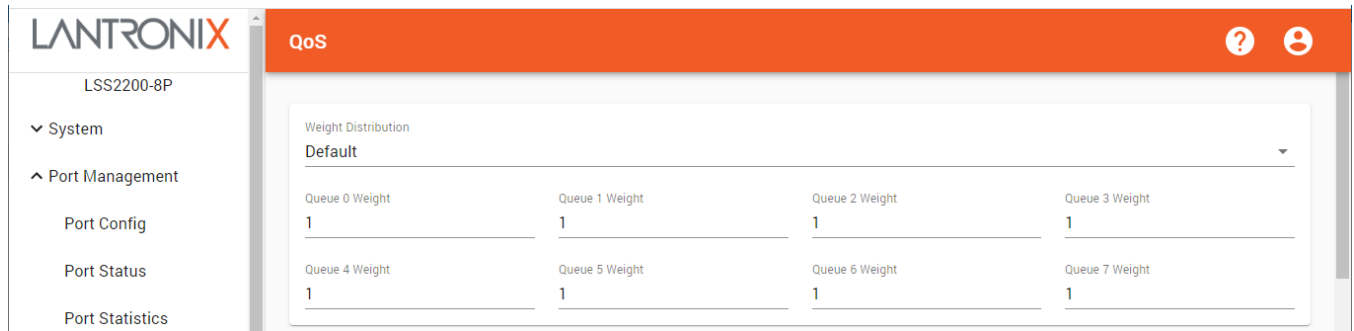
The QoS (Quality of Service) page lets you set and view various QoS parameters.

QoS technology manages data traffic to reduce packet loss, latency and jitter on a network. QoS controls and manages network resources by setting priorities for specific types of data on the network.

Use QoS to meet traffic requirements of sensitive applications (e.g., real-time voice and video) and to prevent degradation of quality caused by delay, jitter, and packet loss.

This page has three sections; Queue Weight Distribution, QoS Configuration, and QoS Port Status as shown and described below.

Queue Weight Distribution



Parameter descriptions:

Weight Distribution: At the dropdown select the desired weight distribution method:

Even : Use even distribution for Quality of Service.

Default : Use default distribution for Quality of Service. This is the default QoS setting.

Custom : Use custom distribution for Quality of Service.



Queue 0 Weight - Queue 7 Weight: Select a valid queue weight for each of up to seven queues. The default is weight 1. The valid weight range is 1-16.

QoS Configuration:

Port	Ingress Limit Enabled	Ingress Limit	Egress Limit Enabled	Egress Limit	Queue Schedule Method	Ingress Priority Mode	Queue Priority	Frame Priority
10GigabitEthernet 1/2	Disabled	100000	Disabled	100000	WRR	Vlan -> IP -> Port	0	0
GigabitEthernet 1/2	Disabled	100000	Disabled	100000	WRR	Port	0	0
GigabitEthernet 1/3	Disabled	100000	Disabled	100000	WRR	Port	0	0
GigabitEthernet 1/4	Disabled	100000	Disabled	100000	WRR	Port	0	0
GigabitEthernet 1/5	Disabled	100000	Disabled	100000	WRR	Port	0	0
GigabitEthernet 1/6	Disabled	100000	Disabled	100000	WRR	Port	0	0
GigabitEthernet 1/7	Disabled	100000	Disabled	100000	WRR	Port	0	0
GigabitEthernet 1/8	Disabled	100000	Disabled	100000	WRR	Port	0	0
10GigabitEthernet 1/1	Disabled	100000	Disabled	100000	WRR	Port	0	0
10GigabitEthernet 1/2	Disabled	100000	Disabled	100000	WRR	Port	0	0

Parameter descriptions:

Port: The table displays a line for each port (e.g., *GigabitEthernet 1/1*).

Ingress Limit Enabled: At the dropdown select ingress limit *Enabled* or *Disabled*. The default is *Disabled*.

Ingress Limit: At the dropdown select a valid ingress limit. The valid range is *1-1000000*. The default is *1000000*.

Egress Limit Enabled: At the dropdown select a valid egress limit *Enabled* or *Disabled*. The default is *Disabled*

Egress Limit: At the dropdown select a valid egress limit. The valid range is *1-1000000*. The default is *1000000*.

Queue Schedule Method: At the dropdown select a valid queue scheduling method (*WRR* or *SP*).

WRR : Weighted Round Robin defines the amount of attention (weight) the queue is given in case of congestion. The weight essentially defines the number of packets taken from queue each time WRR scheduler runs through queues in sequence. WRR is the default setting. WRR ensures that all queues are serviced during each cycle.

SP : Strict Priority ensures service for high-priority traffic. The switch assigns the maximum weights to each queue, causing the queuing mechanism to serve as many packets in one queue as possible before moving to a lower queue.

Ingress Priority Mode CFG: At the dropdown for each port select the ingress priority mode to use:

Port : assign top ingress priority to ports (the default setting).

VLAN -> Port : assign top ingress priority to VLANs, then to ports.

IP -> Port : assign top ingress priority based on IP address, then on port.

VLAN -> IP -> Port : assign top ingress priority based on VLAN, then IP address, and then on port.

IP -> VLAN -> Port : assign top ingress priority based on IP address, then on VLAN, and then on port.

Ingress Priority Mode
CFG

- Port
- Vlan -> Port
- IP -> Port
- Vlan -> IP -> Port
- IP -> Vlan -> Port

Queue Priority: Select a valid queue priority for each port. The valid range is *0-7*. The default is *0*.

Frame Priority: Select a valid frame priority for each port. The valid range is *0-7*. The default is *0*.

QoS Status:

Port	Out Queue 0	Out Queue 1	Out Queue 2	Out Queue 3	Out Queue 4	Out Queue 5	Out Queue 6	Out Queue 7	Queue 0 Count	Queue 1 Count	Queue 2 Count	Queue 3 Count	Queue 4 Count	Queue 5 Count	Queue 6 Count	Queue 7 Count
GigabitEthernet 1/1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
GigabitEthernet 1/2	6816510	0	0	0	0	0	14	0	0	0	0	0	0	0	0	0
GigabitEthernet 1/3	6865466	0	0	9	0	0	11	0	0	0	0	0	0	0	0	0
GigabitEthernet 1/4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
GigabitEthernet 1/5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
GigabitEthernet 1/6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
GigabitEthernet 1/7	406072	0	0	0	0	0	17	0	0	0	0	0	0	0	0	0
GigabitEthernet 1/8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10GigabitEthernet 1/1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10GigabitEthernet 1/2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Parameter descriptions:

Port: The table displays a line for each port (e.g., *GigabitEthernet 1/1*).

Out Queue 0 – Out Queue 7: For each queue and port, displays a count of Out Queues 0-7.

Queue 0 - Queue 7 Count: For each queue and port, displays a count of Queues 0-7.

Buttons:

Cancel: Click to ignore webpage settings.

Apply: Click to save webpage settings to running-config.

Port Management > MAC Address Table

The MAC Address Table page displays various MAC address parameters. The MAC address table is used to map each port to a MAC address, making it efficient to forward traffic directly to a host. The MAC address table consists of two types of entries.

Static entries have higher priority than dynamic entries and remain active; they can be changed or removed by the switch administrator as they are manually added by the switch administrator.

Dynamic entries are added to the table automatically with a process called MAC learning where the switch obtains the source MAC address of each Ethernet frame received on the port.

The screenshot shows the 'MAC Address Table' configuration page. The sidebar on the left lists various network settings, with 'Mac Address Table' selected. The main panel has an orange header with a question mark and user icon. Below the header, there are two settings: 'Aging' set to 'Enabled' and 'Aging Time' set to '300'. A table below lists MAC addresses, their associated VLANs, and ports. The table has three columns: 'MAC Address', 'VLAN', and 'Port'. The first row shows MAC Address '38:F3:AB:EF:83:92', VLAN '1', and Port 'GigabitEthernet 1/1'. The second row shows MAC Address '00:C0:F2:96:08:C1', VLAN '1', and Port 'CPU'. At the bottom right of the table area are 'Cancel' and 'Apply' buttons. A copyright notice 'Copyright © 2023 Lantronix Inc. All rights reserved.' is at the bottom center.

MAC Address	VLAN	Port
38:F3:AB:EF:83:92	1	GigabitEthernet 1/1
00:C0:F2:96:08:C1	1	CPU

Parameter descriptions:

Aging: At the dropdown select *Enabled* or *Disabled* for aging globally. The default is *Disabled*.

Aging Time: Select the length of time that a MAC address entry can remain in the forwarding table. When an entry reaches its aging time, it is 'aged out' and is removed from the table. This essentially cancels frame forwarding to that specific port. The valid range is 4-956 seconds. The default MAC address age timeout is 300 seconds.

MAC Address: Displays the related MAC addresses in the format *11:22:33:44:55:66*.

VLAN: Displays the related VLAN ID.

Port: Displays the related ports (e.g., *GigabitEthernet 1/1*, *GigabitEthernet 1/1*, *CPU*).

Buttons:

Cancel: Click to ignore webpage settings.

Apply: Click to save webpage settings to running-config.

Port Management > DDMI

The DDMI (Digital Diagnostics Monitoring Interface) page lets you view SFP parameters.

The screenshot shows the Lantronix DDMI web interface. The left sidebar contains a navigation menu with the following items: LSS2200-8P, System, Port Management (expanded), Port Config, Port Status, Port Statistics, PVLAN Config, Port VLAN Config, Port Mirroring, Port Security, Virtual Cable Test, Digital IO, LLDP, Spanning Tree, QoS, and Mac Address Table. The main content area is titled 'DDMI' and contains two tables.

Table 1: SFP Parameters

Port	Part Number	Serial Number	Vendor Name	Date Code	Revision
10GigabitEthernet 1/1	TN-GLC-SX-MM	TN32A272	TRANSITION	2014/03/07	1.0
10GigabitEthernet 1/2	TN-SFP-SX	8760926	Transition	2010/10/05	0000

Table 2: Device Status

Port	Type	Alarm	Current Value	High Alarm	Low Alarm	High Warning	Low Warning
10GigabitEthernet 1/1	Tempera	Normal	34.8906	100.0	-40.0	90.0	-35.0
10GigabitEthernet 1/1	Voltage	Normal	3.3468	3.57	3.13	3.47	3.15
10GigabitEthernet 1/1	Bias	Normal	5.832	20.0	0.0	10.0	1.0
10GigabitEthernet 1/1	Tx Powe	Normal	0.2494	0.631	0.0631	0.5012	0.1
10GigabitEthernet 1/1	Rx Powe	Low Alar	0.0	1.0	0.01	0.7943	0.0126
10GigabitEthernet 1/2	Tempera	Normal	0.0	0.0	0.0	0.0	0.0

Parameter descriptions:

Device Information:

Port: The table displays a line for *10GigabitEthernet 1/1* and *10GigabitEthernet 1/2* ports.

Part Number: Displays the SFP part number (PN).

Serial Number: Displays the SFP serial number (SN).

Vendor Name: Displays the SFP manufacturer's name.

Date Code: Displays the SFP date of manufacture.

Revision: Displays the SFP revision number.

Device Status:

Port: The table displays a line for each port (*10GigabitEthernet 1/1* and *10GigabitEthernet 1/2*).

Type: The type of parameter reported on the row (e.g., *Temperature*, *Voltage*, *Bias*, *TX Power*, *RX Power*).

Alarm: The type of alarm (e.g., *High Alarm*, *Normal*, *Low Alarm*, etc.).

Current Value: The existing measurement value reported on the row (e.g., *44.0*, *0.216*).

High Alarm: The existing high alarm measured value reported on the row.

Low Alarm: The existing low alarm measured value reported on the row.

High Warning: The existing high warning measured value reported on the row.

Low Warning: The existing low warning measured value reported on the row.

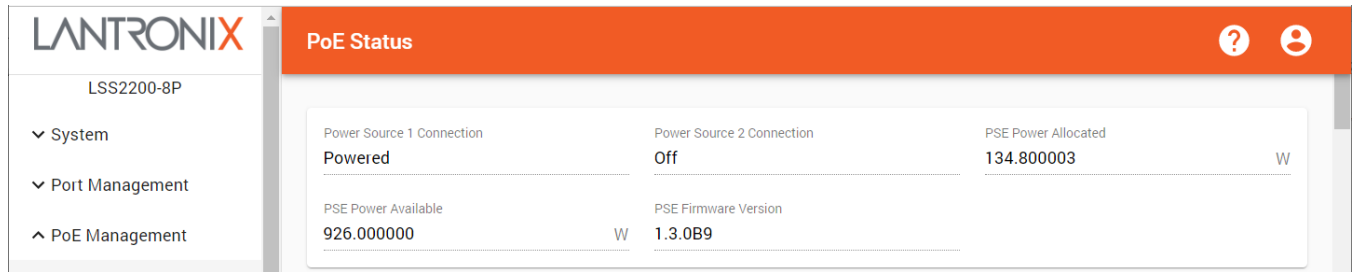
PoE Management

This section lets you view and configure Power over Ethernet functions.

PoE Management > PoE Status

This page lets you view PoE operational status. This page has five sections (Power Source, PD Status, Port Status, APR Status, and Schedule Status) as shown and described below.

PoE Power Source:



Parameter descriptions:

Power Source 1 Connection : Displays the current status of power source 1 (e.g., *Powered* or *Off*).

Power Source 2 Connection : Displays the current status of power source 2 (e.g., *Powered* or *Off*).

PSE Power Allocated : Displays the amount of PSE power that is currently allocated by the switch in Watts.

PSE Power Available : Displays the amount of PSE power that is currently available to be delivered by the switch in Watts.

PSE Firmware Version : Displays the current version of PSE firmware (e.g., *1.3.0B9*).

PoE Management > PoE Status > PD Status:

LSS2200-8P											
<ul style="list-style-type: none"> System Port Management PoE Management <ul style="list-style-type: none"> PoE Status PoE Config PoE Auto Power Reset PoE Scheduler SNMP Notifications Maintenance ConsoleFlow Lantronix Provision Manager 											
Port Name	PD CLASS	Power Used	Current Used	PD Voltage	Temperature	Power Requested	Power Allocated				
GigabitEthernet 1/8	-	0 W	0 mA	0.0 V	32.5 C	0 W	0 W				
GigabitEthernet 1/7	2	1.9 W	35 mA	56.26 V	33.75 C	15 W	0 W				
GigabitEthernet 1/6	4	6.7 W	119 mA	56.39 V	33.75 C	60 W	0 W				
GigabitEthernet 1/5	3	3.4 W	62 mA	56.07 V	35.0 C	15 W	0 W				
GigabitEthernet 1/4	2	1.9 W	34 mA	56.46 V	33.75 C	15 W	0 W				
GigabitEthernet 1/3	-	0 W	0 mA	0.0 V	33.75 C	0 W	0 W				
GigabitEthernet 1/2	-	0 W	0 mA	0.0 V	35.0 C	0 W	0 W				
GigabitEthernet 1/1	-	0 W	0 mA	0.0 V	35.0 C	0 W	0 W				

Port Name: The table displays a line for each port (e.g., *GigabitEthernet 1/1*).

PD CLASS: Displays the powered device’s PoE class (1-8). Each PD is assigned a class that defines the maximum power the PD will use. The PD class column shows each PD’s class. The PD Classes are:

Class 1: Max. power 4.0 W	Class 5: Max. power 45 W
Class 2: Max. power 7.0 W	Class 6: Max. power 60 W
Class 3: Max. power 15.4 W	Class 7: Max. power 75 W
Class 4: Max. power 30.0 W	Class 8: Max. power 90 W

Power Used: Shows how much power the PD currently is using in Watts.

Current Used: Displays the amount of current the PD is using in milliamps.

PD Voltage: Displays the PD’s voltage in Volts.

Temperature: Displays the current temperature of the PSE port on the LSS2200-8P in degrees Celsius.

Power Requested: Displays the requested amount of power the PD wants to be reserved in Watts.

Power Allocated: Displays the amount of power the switch has allocated for the PD.

PoE Management > PoE Status > Port Status:

This section lets you view the current PoE Port Status.

LANTRONIX		PoE Status	
LSS2200-8P		Port Name	Port Status
System		GigabitEthernet 1/8	No-PD-Detected
Port Management		GigabitEthernet 1/7	PD-Detected-4-Pair-IEEE-802.3bt-Single-Signature
PoE Management		GigabitEthernet 1/6	PD-Detected-4-Pair-IEEE-802.3bt-Single-Signature
PoE Status		GigabitEthernet 1/5	PD-Detected-4-Pair-IEEE-802.3bt-Single-Signature
PoE Config		GigabitEthernet 1/4	PD-Detected-4-Pair-IEEE-802.3bt-Single-Signature
PoE Auto Power Reset		GigabitEthernet 1/3	No-PD-Detected
PoE Scheduler		GigabitEthernet 1/2	No-PD-Detected
SNMP		GigabitEthernet 1/1	No-PD-Detected
Notifications			
Maintenance			
ConsoleFlow			
Lantronix Provision Manager			

Parameter descriptions:

Port Name: Displays a switch port on each row (e.g., *GigabitEthernet 1/1*).

Port Status: Displays the PoE status of the port. The PoE PSE firmware supports these port status values:

- **Disabled-PHO:** PoE Hardware Override is active (DIP switch setting).
- **Port-Off:** PoE is configured as disabled for the port or for the switch as a whole.
- **No-PD-Detected:** the switch did not detect any PD status.
- **unknown:** the switch was unable to detect a specific PoE status.
- **PD-Detected-2-Pair-IEEE-802.3bt-Single-Signature.**
- **PD-Detected-4-Pair-IEEE-802.3bt-Single-Signature.**
- **PD-Forced :** PoE is configured to deliver power in Forced mode (ignoring PD classification). In Forced mode the switch port will power up the linked PD without any detect/negotiate mechanism so it is important that you know what the PD is capable of accepting to prevent damage.

PoE Management > PoE Status > APR Status:

This section lets you view Auto Power Reset (APR) Status parameters.

Port Name	APR Status
GigabitEthernet 1/8	Port Disabled - APR Failure - Discovery failed after 20 minutes, please verify configuration
GigabitEthernet 1/7	Port Disabled - APR Failure - Discovery failed after 20 minutes, please verify configuration
GigabitEthernet 1/6	Port Disabled - APR Failure - Discovery failed after 20 minutes, please verify configuration
GigabitEthernet 1/5	Port Disabled - APR Failure - Discovery failed after 20 minutes, please verify configuration
GigabitEthernet 1/4	Monitoring - Duration: 9922s Consecutive Failures: 0 Failure Events: 0
GigabitEthernet 1/3	Port Disabled - APR Failure - Discovery failed after 20 minutes, please verify configuration
GigabitEthernet 1/2	APR Failure - Discovery failed after 20 minutes, please verify configuration
GigabitEthernet 1/1	Off

Parameter descriptions:

Port Name: Displays a switch port on each row (e.g., *GigabitEthernet 1/1*).

APR Status: Displays the status of the PoE Auto Power Reset:

Off : PoE APR is disabled.

On : PoE APR is enabled.

Monitoring - Duration: 0s Consecutive Failures: 0 Failure Events: 0 : PoE APR monitoring has begun.

Discovery Phase 1 - Duration: 0s : PoE discovery phase 1 has begun.

Port Disabled - APR Failure - Discovery failed after 20 minutes, please verify configuration: the PoE APR discovery failed after 20 minutes; check the port config.

APR Failure - Discovery failed after 20 minutes, please verify configuration: the PoE APR discovery failed after 20 minutes; check the APR config.

PoE Management > PoE Status > Schedule Status:

This section lets you view PoE Schedule parameters.

Port Name	Schedule Status
GigabitEthernet 1/8	RbtSched1: Off - Disabled by service
GigabitEthernet 1/7	RbtSched1: Off - Disabled by service
GigabitEthernet 1/6	RbtSched2: Off - Disabled by service
GigabitEthernet 1/5	RbtSched2: Off - Disabled by service
GigabitEthernet 1/4	RbtSched1: Running - Current PoE State: On Next event: Reset, Monday at 12:30
GigabitEthernet 1/3	Off
GigabitEthernet 1/2	RbtSched1: Running - Current PoE State: On Next event: Reset, Monday at 12:30
GigabitEthernet 1/1	RbtSched1: Running - Current PoE State: On Next event: Reset, Monday at 12:30

Parameter descriptions:

Port Name: Displays a switch port on each row (e.g., *GigabitEthernet 1/1*).

Schedule Status: Displays the status of the PoE Event Schedule. There are four possible status messages:

1. *Off*
2. *<schedule name>: Off - Disabled by service*
3. *<schedule name>: Running - Current PoE State: [Off/On/Resetting/Switching] Next event: [Off/On/Reset], [Day of the week] at [hour]:[minute]*
4. *<schedule name>: Empty Schedule*

Off: no schedule has been applied to this port.

Off - Disabled by service: PoE has been disabled by another service (e.g.: APR or PoE Mode) so the current schedule is disabled.

Running - Current PoE State: the applied schedule is running. Current PoE State is whether PSE is currently off, on, resetting (power cycling the port), or switching to another schedule. Next event shows what will happen next and when.

Empty Schedule: the currently applied schedule has no events associated with it so the scheduler will not affect the port.

PoE Management > PoE Config

This page lets you set Power over Ethernet parameters.



Warning: Attached Power Supply’s wattage must be set in the Power Supply 1 and/or Power Supply 2 field(s) before the PSE ports will supply power. See “Power Supply Information” in the Install Guide.

LANTRONIX PoE Config

LSS2200-8P

Ultra-fast PoE: Enabled | Power Supply 1: 100 W | Power Supply 2: 675 W

ID	PoE Mode	Max Power	Priority	Operation Mode	Schedule
GigabitEthernet 1/1	Enabled	45	W	Low	IEEE-802.3at
GigabitEthernet 1/2	Enabled	45	W	Critical	IEEE-802.3bt
GigabitEthernet 1/3	Enabled	25	W	High	IEEE-802.3bt
GigabitEthernet 1/4	Enabled	20	W	High	IEEE-802.3bt
GigabitEthernet 1/5	Enabled	30	W	Low	IEEE-802.3bt
GigabitEthernet 1/6	Enabled	25	W	Low	IEEE-802.3bt
GigabitEthernet 1/7	Enabled	40	W	Low	IEEE-802.3af
GigabitEthernet 1/8	Enabled	45	W	Critical	IEEE-802.3bt

Copyright © 2023 Lantronix Inc. All rights reserved.

Parameter descriptions:

Ultra-fast PoE: At the dropdown select *Enabled* or *Disabled* for Ultra-fast PoE support. Ultra-fast PoE improves PoE startup time; it provides PoE output to attached PDs within five seconds after a cold start. The default is *Enabled*. **Note:** When PHO is in use or is going to be used, the Ultra-Fast PoE function must be enabled. Since PHO can be enabled while the unit is off, you must enable Ultra-Fast PoE before enabling PHO. (**Note:** PHO is currently Disabled by default; do not override until fully supported).

Power Supply 1: Lets you set and view the power output of PS1 in Watts. The valid range is 0 - 1600 Watts, where 0 means no PSU attached for that Power Supply input.

Power Supply 1 and Power Supply 2: The power supply wattage must be set according to user's selected power supply capability (see the “Setting the Power Supply Values in Switch Software” section in the Install Guide for details on power requirements).

Power Supply 2: Lets you set and view the power output of PS2 in Watts. The valid range is 0 - 1600 Watts, where 0 means no PSU attached for that Power Supply input.

Note: The LSS2200-8P unit consumes approximately 30 Watts of power, and that level is taken from the configured value. Each power supply that is present and required for power delivery to PDs must be set for a power output greater than 30W. Setting power output to a value that is less than the expected PD load + 30W might cause the PD to lose power.

For example, if Power Supply 1 is used and must supply an expected PD load of 60W, then Power Supply 1 must be configured for 90W or greater, since the switch uses 30W from that value.

ID: The table displays a line for each port (e.g., *GigabitEthernet 1/1*).

PoE Mode: At the dropdown select the desired PoE mode for each port (*Enabled*, *Disabled*, or *Force*). The default is *Enabled*. In *Force* mode the switch port will power up the linked PD without any detect/negotiate mechanism so it is important that you know that the PD is capable of accepting power to prevent damage.

PoE Mode

Enabled
Disabled
Force

Max Power: Max Power is a deprecated field; it is not needed and will be removed in future releases. Leave at 0.

Setting the Power Supply Values in Switch Software:

CAUTION: Always match the PSx input supply to the Power Supply 1 and Power Supply 2 software setting. Mismatching will cause the LSS2200-8P to think it can draw more power from the external supply than it is capable of providing and results could be detrimental.

Note: The power supply wattage value(s) must be manually set in the software by the user to match the connected external power supply(ies). The LLSS2200-8P uses this wattage as the “PSE Power Available” to determine if enough power is available during PoE PD classification to power up connected PDs. See additional details on power requirements in the Install Guide.

Power Supply 1 and Power Supply 2 wattage must be set according to power supply capability (see the “Setting the Power Supply Values in Switch Software” section in the Install Guide for details on power requirements).

Priority: At the dropdown select the desired operating priority in terms of power for each port. The three levels of power priority are *Low*, *High* and *Critical*. The priority is used in the case where the remote devices requires more power than the power supply can deliver. In this case the port with the lowest priority will be turned off starting from the port with the highest port number. The default setting is *Low* priority.

Priority

Low
High
Critical

Operation Mode: At the dropdown select the desired PoE operation mode:

IEEE-802.3af : Enables PoE IEEE 802.3af for the port.

IEEE-802.3at : Enables PoE IEEE 802.3at for the port.

IEEE-802.3bt : Enables PoE IEEE 802.3bt for the port (default). **Note** that PoE++ requires >54V.

IEEE 802.3bt is the default and should be used with any IEEE 802.3af/at/bt device. For non-IEEE 802.3af/at/bt compliant devices, change **PoE Mode** to *Force* and leave **Max Power** at *0W*.

Operation Mode

IEEE-802.3af
IEEE-802.3at
IEEE-802.3bt

Schedule: At the dropdown select a schedule instance for PoE Scheduling. You must first define one or more PoE schedules on the PoE Scheduler page (see below).

Buttons:

Cancel: Click to ignore webpage settings to running-config.

Apply: Click to save webpage settings to running-config.

PoE Management > PoE Auto Power Reset

This page allows you to configure the automatic power reset function on a per-port basis. This feature lets you specify the auto detection parameters to check the link status between switch PoE ports and PDs. When it detects a failed connection, the switch will reboot the remote PD automatically.

Port	Enable	Ping IP Address	Interval	Ping Retries	Failure Action
GigabitEthernet 1/1	Enabled	0.0.0.0	10 s	3	Log and Trap
GigabitEthernet 1/2	Enabled	192.168.60.6	10 s	3	Reset, Log and Trap
GigabitEthernet 1/3	Enabled	192.168.60.6	10 s	3	Reset, Log and Trap
GigabitEthernet 1/4	Enabled	192.168.60.6	10 s	3	Reset, Log and Trap
GigabitEthernet 1/5	Enabled	192.168.60.6	10 s	3	Log and Trap
GigabitEthernet 1/6	Enabled	192.168.60.6	10 s	3	Log and Trap
GigabitEthernet 1/7	Enabled	0.0.0.0	10 s	3	Log and Trap
GigabitEthernet 1/8	Enabled	192.168.60.6	10 s	3	Reset, Log and Trap

Buttons: Cancel, Apply

Copyright © 2023 Lantronix Inc. All rights reserved.

Parameter descriptions:

Port: The table displays a line for each port (e.g., *GigabitEthernet 1/1*).

Enable: At the dropdown select *Enabled* or *Disabled* for automatic power reset.

Ping IP Address: Enter the IPv4 IP address of the PD to be pinged.

Interval: The switch will send a ping to the PD each interval time. The valid range is 10-120 seconds.

Ping Retries: When the PoE port can't ping the PD, it will try to send detection again. By default, after the third unsuccessful try, it will trigger the configured failure action. The valid range is 1-5 retry attempts.

Failure Action: At the dropdown select the action for the switch to take if the configured ping attempts fail.

Log and Trap: Log and trap the ping failure.

Reset, Log and Trap: Reset the PD and log and trap the ping failure.

Buttons:

Cancel: Click to cancel webpage settings.

Apply: Click to save webpage settings to running-config.

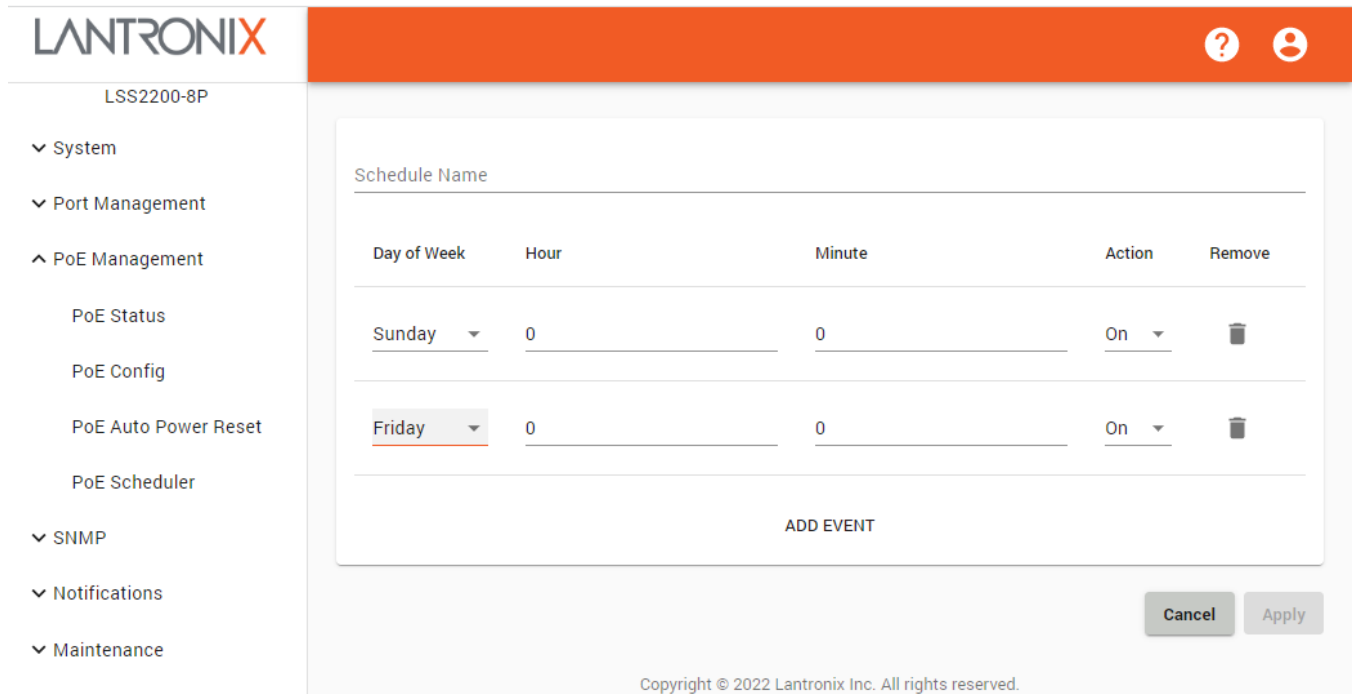
PoE Management > PoE Scheduler

This page lets you define 1-16 PoE scheduled events/actions. You can then modify and delete existing events.

A PoE Schedule is cyclic on a weekly basis. This means if you add a single 'On' event to a schedule, the PSE will always be 'On'. A single 'Off' event would result in an always 'Off' PSE state. A schedule with a single 'Reset' event would be a practical schedule ensuring a weekly reboot of a device at the specified time. Otherwise, a schedule should have at least one 'On' event and one 'Off' event to have the schedule manage the port.

When the schedule is applied, the scheduler will determine the current expected state of the port and set it immediately. Setting the PoE Mode to 'Disabled' will completely override the schedule and the PSE will always be off. To use a schedule, the PoE Mode must be 'Enabled' or 'Force'.

On the initial page, click the + ADD SCHEDULE button and then click the + ADD EVENT button to display the PoE Scheduler page:



Parameter descriptions:

Schedule Name: Enter a name for this schedule instance.

Day of Week: At the dropdown select the day (Sunday - Saturday) for the configured action to be scheduled.

Hour: Enter or select the desired hour (0-23).

Minute: Enter or select the desired minute (0-59).

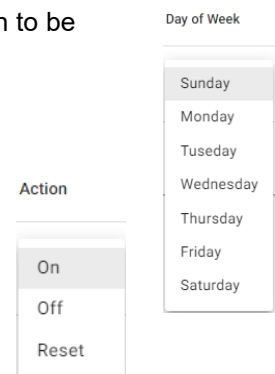
Action: At the dropdown select the action to be scheduled:

On : Turn the attached device on at the scheduled time/day.

Off : Turn the attached device off at the scheduled time/day.

Reset : Reset the attached device at the scheduled time/day.

Remove: Click the  icon in the Remove column of a row to delete the instance.

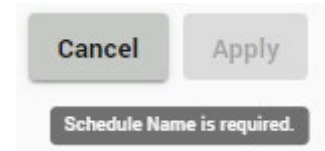


Buttons:

Cancel: Click to cancel webpage settings.

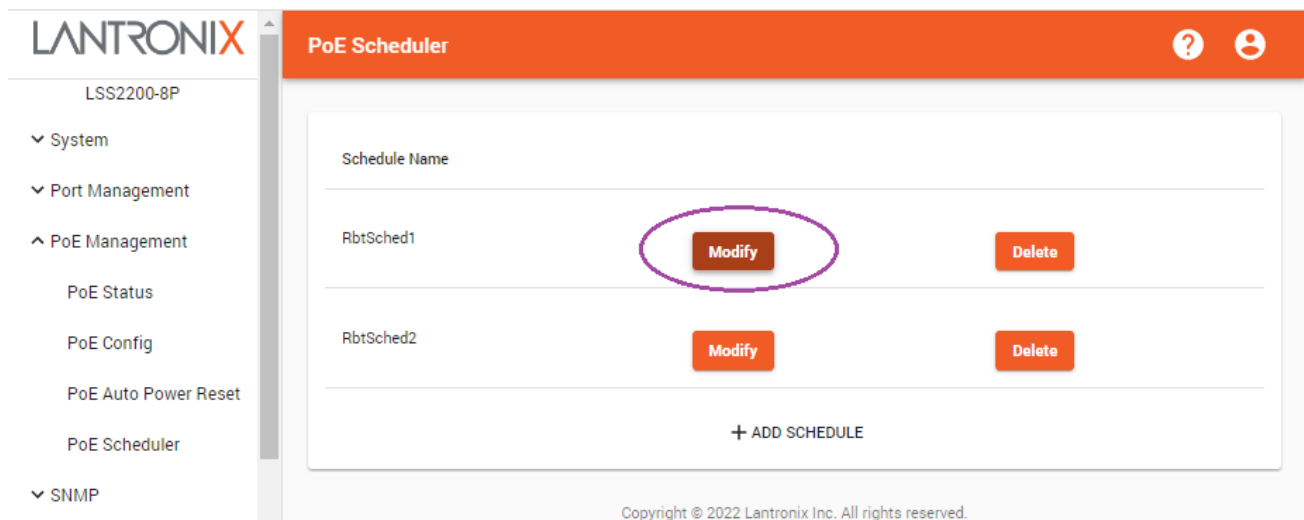
Apply: Click to save webpage settings to running-config.

Messages: *Schedule Name is required.:* a conditional tooltip displays when you hover the Apply button when the Schedule Name is not provided.

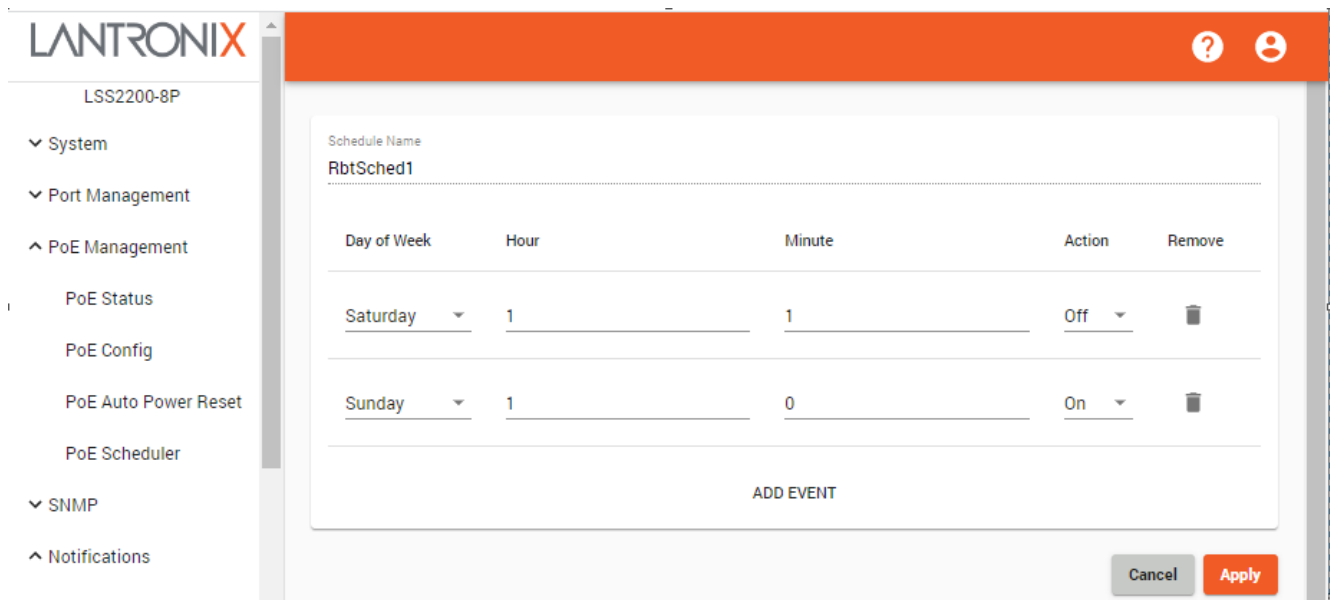


Modify a Scheduled Event

To modify an existing schedule, click the **Modify** button.



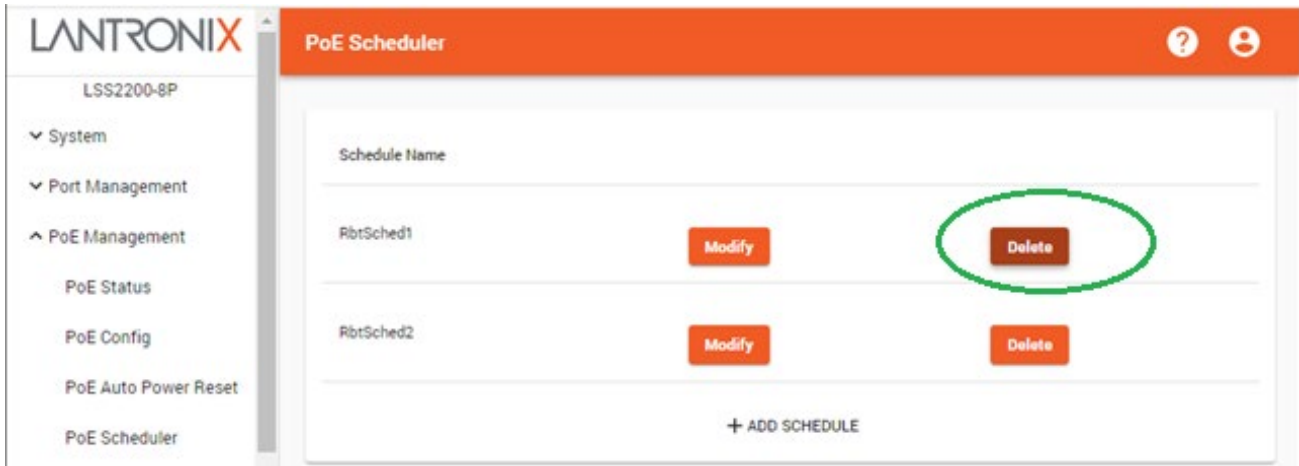
At the modify page, enter or select the desired changes and then click the **Apply** button.



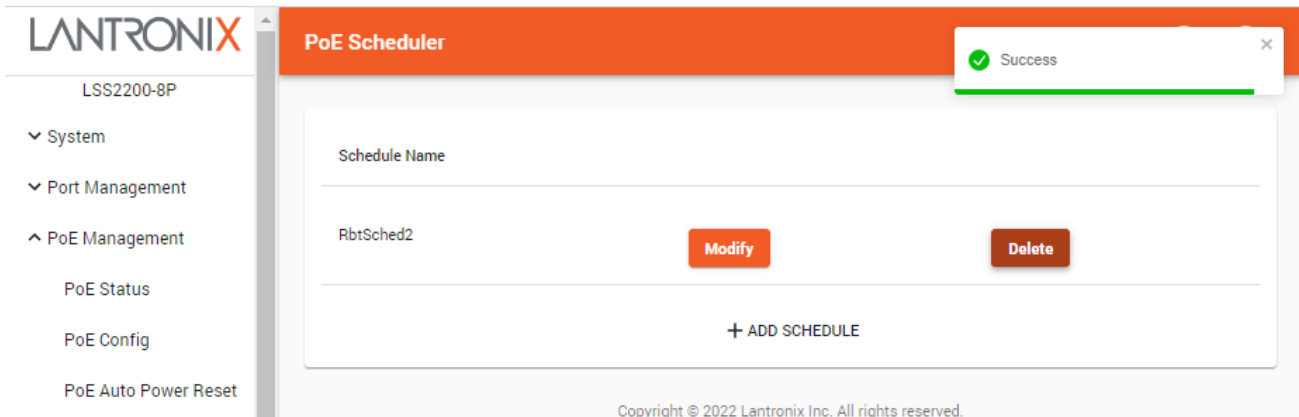
You can click the **Cancel** button to cancel the modify operation and return to the PoE Scheduler page.

Delete a Scheduled Event

To delete an existing schedule, click the **Delete** button.



Wait for the scheduled event to be deleted successfully:



Buttons:

Cancel: Click to ignore changes made to the webpage.

Modify: Click to edit the selected entry.

Delete: Click to remove the unsaved entry from the table.

SNMP

This section lets you set SNMP parameters.

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. SNMP is a protocol used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the Management Information Base (MIB), described in the form of SMI syntax. An SNMP agent runs on the switch to respond to requests issued by the SNMP manager.

SNMP is basically passive, except for issuing trap information. The LSS2200-8P supports a switch to turn the SNMP agent on or off. If you select Enabled at the SNMP Enabled dropdown, the SNMP agent will start up. All supported MIB OIDs can be accessed via the SNMP manager. If SNMP Enabled is set to “Disabled”, the SNMP agent will be de-activated, and requests sent to the switch will fail due to no response.

SNMP > SNMP

This page lets you set SNMP Configuration parameters. Click the + ADD IP button to display a new row in the table to configure.

The screenshot shows the Lantronix web interface for the LSS2200-8P device. The left sidebar contains a navigation menu with the following items: System, Port Management, PoE Management, SNMP (expanded), SNMPv2 Communities, SNMPv3 Users, SNMPv3 Views, Notifications, Maintenance, ConsoleFlow, and Lantronix Provision Manager. The main content area is titled 'SNMP' and contains the following configuration fields:

- SNMP Enabled:** A dropdown menu currently set to 'Disabled'.
- System Name:** A text field containing 'LSS2200-8P'.
- System Contact:** A text field containing 'TomT'.
- System Location:** A text field containing 'Plymouth_MN'.
- Enable Auth Trap:** A dropdown menu currently set to 'Enabled'.
- Enable Link Up Down Trap:** A dropdown menu currently set to 'Enabled'.

Below the configuration fields is a table with the following structure:

IP	Delete
1.2.3.4	

At the bottom of the table is a '+ ADD IP' button. In the top right corner of the main content area, there is a green success message: 'Success'.

Parameter descriptions:

SNMP Enabled: At the dropdown select *Enabled* or *Disabled* for SNMP global operation. The default is *Disabled*.

System Name: Enter a name for the switch (e.g., *LSS2200-8P*).

System Contact: Enter a contact for the switch.

System Location: Enter the location of the switch.

Enable Auth Trap: At the dropdown select *Enabled* for the `authenticationFailure` trap. The default is *Disabled*.

Enable Link Up Down Trap: At the dropdown select *Enabled* for the trap for `linkUp` and `linkDown` traps. The default is *Disabled*.


IP: Enter the IP address for the SNMP parameters.

Buttons:

Cancel: Click to ignore webpage changes.

Apply: Click to save webpage settings to running-config.

+ ADD IP: Click the button to add an IP address to the table, then enter parameters in the displayed fields:

Delete: Click the  icon in the Delete column of a row to delete the instance from the table and the system.

SNMP > SNMPv2 Communities

This page lets you set SNMPv2 communities parameters in the SNMPv2 Communities Configuration table. At the default page click the + ADD ROW button to display an additional row in the table for configuration.

The screenshot displays the LANTRONIX web interface for configuring SNMPv2 Communities. The main content area is titled "SNMPv2 Communities Configuration" and contains a table with the following structure:

Name	Host Access	Restrict OID	
public			

Below the table is a "+ ADD ROW" button. At the bottom right of the configuration area are "Cancel" and "Apply" buttons. The left sidebar shows the navigation menu with "SNMPv2 Communities" selected.

Parameter descriptions:

Name: The SNMPv2 community name. By default, one instance exists, named "Public".

Host Access: Enter an SNMP server IP address or host name.

Restrict OID: Enter an SNMP OID to which you want to restrict access in the format 1.3.6.1.6.3.1.2.2.11.

Buttons:

Cancel: Click to ignore webpage changes.

Apply: Click to save webpage settings to running-config.

+ ADD ROW: Click the button to add an IP address to the table, then enter parameters in the displayed fields:

Delete: Click the icon in the Delete column of a row to delete the instance from the table and the system.

Messages:

400 Error: Invalid SNMP object ID: 1.3.6.1.6

SNMP > SNMPv3 Users

This page lets you set SNMPv3 users' parameters in the SNMPv3 User Configuration table.

At the default page click the + ADD ROW button to display an additional row in the table for configuration.

Parameter descriptions:

User Name: Enter the SNMPv3 user's name.

View: At the dropdown select an existing SNMPv3 view (see below).

Security Level: At the dropdown select the level of security required in order to login:

No Auth No Priv means this user can login without authentication and privacy protocol settings being configured for that user.

Auth No Priv means authentication but no privacy protocol settings must be configured in order for this user to be able to login.

Auth Priv means both authentication and privacy protocol settings must be configured in order for this user to be able to login.

Security Level

Auth Protocol: At the dropdown select the authentication protocol to which this entry should belong. Possible authentication protocols are:

None: No authentication protocol.

MD5: This user will use the MD5 authentication protocol.

SHA: This user will use the SHA authentication protocol.

Auth Key: Enter a string identifying the authentication password key. For MD5 authentication protocol, the allowed string length is 8-32 characters. For SHA authentication protocol, the allowed string length is 8-40 characters. The allowed content is ASCII characters 33-126.

Priv Protocol: At the dropdown select the privacy protocol that this entry should belong to. Possible privacy protocols are:

None: No privacy protocol.

DES: An optional flag to indicate that this user uses DES authentication protocol.

AES: An optional flag to indicate that this user uses AES authentication protocol.

Priv Key: Enter a string identifying the privacy password key. The allowed string length is 8-32 characters, and the allowed content is ASCII characters 33-126.

Buttons:

Cancel: Click to ignore webpage changes.

Apply: Click to save webpage settings to running-config.

+ ADD ROW: Click the button to add an IP address to the table, then enter parameters in the displayed fields:

Delete: Click the  icon in the Delete column of a row to delete the instance from the table and the system.

Definitions:

MD5 (Message-Digest algorithm 5) is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in IETF RFC 1321 (the MD5 Message-Digest Algorithm).

SHA (Secure Hash Algorithm) was designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

DES (Data Encryption Standard) provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a "key".

AES (Advanced Encryption Standard) is the encryption key protocol applied in the 802.11i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

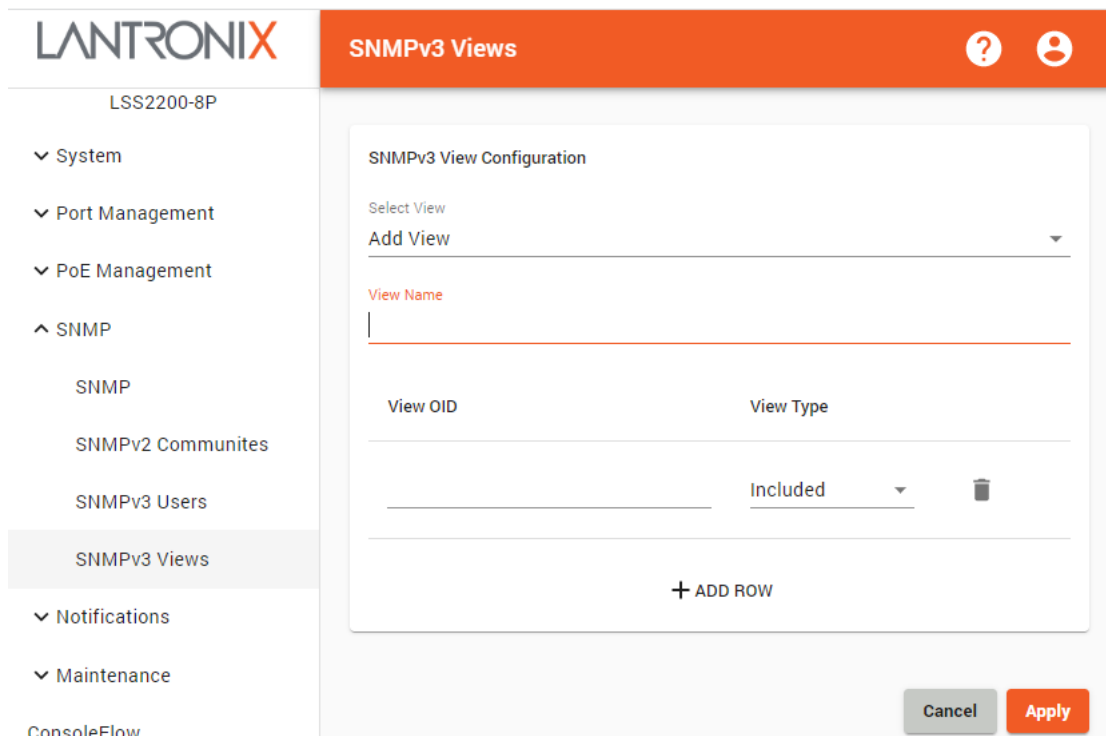
SNMP > SNMPv3 Views

This page lets you configure SNMPv3 Views.

In SNMPv3, a view controls the scope of what is visible to users associated with that view. A view is defined as a list of OIDs that are included and/or a list of OIDs that are excluded from the view. Each OID may represent any portion of the MIB, from a leaf node (single object) to any sub-tree including the top level (root of the MIB tree). This allows for controlling a wide range of scope visibility, from very broad to very narrow. When combined with multiple SNMPv3 users, it is possible to set different levels of visibility to different users.



From the default page at the Select View dropdown select Add View and click the + button to display an initial SNMPv3 View instance to configure.



Parameter descriptions:

View Name: Enter a name for this SNMPv3 View instance.

View OID: Enter an OID (Object Identifier) for the SNMPv3 View instance.

View Type: At the dropdown select the type of view to use (*Included* or *Excluded*).

View Type

Included


Excluded

Buttons:

Cancel: Click to ignore webpage changes.

Apply: Click to save webpage settings to running-config.

+ ADD ROW : Click the icon to add an IP address to the table, then enter parameters in the displayed fields.

Delete: Click the  icon in the Delete column of a row to delete the instance from the table and the system.

Notifications

This section lets you set and view alarms and BLE parameters and manage users.

Notifications > Alarms

This page lets you view active alarms.

Alarm	Message	State	Timestamp	Level
10GigabitEthernet-1/1-Temperature-high-	Temperature 35.63671875 is above threshl	active	2023-02-01T12:24:24+00:00	error
10GigabitEthernet-1/1-Voltage-high-alarrr	Voltage 3.3425 is above threshold	active	2023-02-01T12:24:24+00:00	error
10GigabitEthernet-1/1-Bias-high-alarm	Bias 82.82 is above threshold	active	2023-02-01T12:24:24+00:00	error
10GigabitEthernet-1/1-Tx-Power-high-alar	Tx Power 1.5346 is above threshold	active	2023-02-01T12:24:24+00:00	error
10GigabitEthernet-1/1-Rx-Power-high-alar	Rx Power 0.0 is above threshold	active	2023-02-01T12:24:24+00:00	error
10GigabitEthernet-1/2-Temperature-high-	Temperature 32.53125 is above threshold	active	2023-02-01T12:28:31+00:00	error
10GigabitEthernet-1/2-Voltage-high-alarrr	Voltage 3.3963 is above threshold	active	2023-02-01T12:28:31+00:00	error
10GigabitEthernet-1/2-Bias-high-alarm	Bias 38.984 is above threshold	active	2023-02-01T12:28:31+00:00	error
10GigabitEthernet-1/2-Tx-Power-high-alar	Tx Power 1.6922 is above threshold	active	2023-02-01T12:28:31+00:00	error
10GigabitEthernet-1/2-Rx-Power-high-alar	Rx Power 0.0 is above threshold	active	2023-02-01T12:28:31+00:00	error

Copyright © 2023 Lantronix Inc. All rights reserved.

Parameter descriptions:

Alarm Status:

Alarm: Displays the alarm raised (e.g., *10GigabitEthernet-1/1-Voltage-high-alarm*).

Message: Displays the alarm message (e.g., *Voltage 3.348 is above threshold*).

State: Displays the alarm state (e.g., *active*).

Timestamp: Displays the date and time the alarm occurred (e.g., *2023-02-01T12:28:31+00:00*).

Level: Displays the alarm level (e.g., *error, warning*).

Notifications > Alarm Config

This page lets you enable and disable alarms.

Alarms conditions are triggered and cleared by specific events. You can configure alarms to be disabled. The switch maintain a list of active alarms that can be retrieved, and each alarm event (raise or clear) gets logged. An alarm example: *SFP DDMI item exceeds a threshold value*.

Alarm	Admin State
10GigabitEthernet-1/1-Temperature-high-alarm	Enabled
10GigabitEthernet-1/1-Temperature-low-alarm	Enabled
10GigabitEthernet-1/1-Temperature-high-warning	Enabled
10GigabitEthernet-1/1-Temperature-low-warning	Enabled
...	...
port-security-10GigabitEthernet-1/1-limit-reached	Enabled
port-security-10GigabitEthernet-1/2-shutdown	Enabled
port-security-10GigabitEthernet-1/2-limit-reached	Enabled
CPU-Temperature	Enabled

Parameter descriptions:

Alarm: Displays a table of all available alarms which you can enable or disable individually.

Admin State: At the dropdown select *Enabled* or *Disabled* for each individual Alarm listed. All Alarms are *Enabled* by default.

Buttons:

Cancel: Click to ignore webpage changes.

Apply: Click to save webpage settings to running-config.

Configurable Alarms:

10GigabitEthernet-1/1-Temperature-high-alarm
10GigabitEthernet-1/1-Temperature-low-alarm
10GigabitEthernet-1/1-Temperature-high-warning
10GigabitEthernet-1/1-Temperature-low-warning
10GigabitEthernet-1/1-Voltage-high-alarm
10GigabitEthernet-1/1-Voltage-low-alarm
10GigabitEthernet-1/1-Voltage-high-warning
10GigabitEthernet-1/1-Voltage-low-warning
10GigabitEthernet-1/1-Bias-high-alarm
10GigabitEthernet-1/1-Bias-low-alarm
10GigabitEthernet-1/1-Bias-high-warning
10GigabitEthernet-1/1-Bias-low-warning
10GigabitEthernet-1/1-Tx-Power-high-alarm
10GigabitEthernet-1/1-Tx-Power-low-alarm
10GigabitEthernet-1/1-Tx-Power-high-warning
10GigabitEthernet-1/1-Tx-Power-low-warning
10GigabitEthernet-1/1-Rx-Power-high-alarm
10GigabitEthernet-1/1-Rx-Power-low-alarm
10GigabitEthernet-1/1-Rx-Power-high-warning
10GigabitEthernet-1/1-Rx-Power-low-warning
10GigabitEthernet-1/2-Temperature-high-alarm
10GigabitEthernet-1/2-Temperature-low-alarm
10GigabitEthernet-1/2-Temperature-high-warning
10GigabitEthernet-1/2-Temperature-low-warning
10GigabitEthernet-1/2-Voltage-high-alarm
10GigabitEthernet-1/2-Voltage-low-alarm
10GigabitEthernet-1/2-Voltage-high-warning
10GigabitEthernet-1/2-Voltage-low-warning
10GigabitEthernet-1/2-Bias-high-alarm
10GigabitEthernet-1/2-Bias-low-alarm
10GigabitEthernet-1/2-Bias-high-warning
10GigabitEthernet-1/2-Bias-low-warning
10GigabitEthernet-1/2-Tx-Power-high-alarm
10GigabitEthernet-1/2-Tx-Power-low-alarm
10GigabitEthernet-1/2-Tx-Power-high-warning
10GigabitEthernet-1/2-Tx-Power-low-warning
10GigabitEthernet-1/2-Rx-Power-high-alarm
10GigabitEthernet-1/2-Rx-Power-low-alarm
10GigabitEthernet-1/2-Rx-Power-high-warning
10GigabitEthernet-1/2-Rx-Power-low-warning
loop-shutdown-GigabitEthernet-1/1
loop-shutdown-GigabitEthernet-1/2
loop-shutdown-GigabitEthernet-1/3
loop-shutdown-GigabitEthernet-1/4
loop-shutdown-GigabitEthernet-1/5
loop-shutdown-GigabitEthernet-1/6
loop-shutdown-GigabitEthernet-1/7
loop-shutdown-GigabitEthernet-1/8
loop-shutdown-10GigabitEthernet-1/1
loop-shutdown-10GigabitEthernet-1/2
port-security-GigabitEthernet-1/1-shutdown
port-security-GigabitEthernet-1/1-limit-reached
port-security-GigabitEthernet-1/2-shutdown
port-security-GigabitEthernet-1/2-limit-reached
port-security-GigabitEthernet-1/3-shutdown
port-security-GigabitEthernet-1/3-limit-reached
port-security-GigabitEthernet-1/4-shutdown
port-security-GigabitEthernet-1/4-limit-reached
port-security-GigabitEthernet-1/5-shutdown
port-security-GigabitEthernet-1/5-limit-reached
port-security-GigabitEthernet-1/6-shutdown
port-security-GigabitEthernet-1/6-limit-reached
port-security-GigabitEthernet-1/7-shutdown
port-security-GigabitEthernet-1/7-limit-reached
port-security-GigabitEthernet-1/8-shutdown
port-security-GigabitEthernet-1/8-limit-reached
port-security-10GigabitEthernet-1/1-shutdown
port-security-10GigabitEthernet-1/1-limit-reached
port-security-10GigabitEthernet-1/2-shutdown
port-security-10GigabitEthernet-1/2-limit-reached
CPU-Temperature

Notifications > Syslog

This page lets you set System log parameters.

Parameter descriptions:

Global Settings:

Buffer Size: Enter or select the desired size of the Syslog buffer. The default is 64 bytes.

Output Level: At the dropdown select the level of Syslog output to be reported. Note that when you configure the logging severity, that severity level applies to the internal log and to log message forwarding to a syslog server. The syslog output levels are:

Emergency: The system is unusable (e.g., panic condition).

Alert: Action must be taken immediately. A condition that should be corrected immediately, such as a corrupted system database.

Critical: Critical conditions (e.g., hard device error).

Error: The system log entry is at error level.

Warning: The system log entry is at warning level (default).

Notice: Normal but significant conditions. Conditions that are not error conditions, but that may require special handling.

Info: The system log entry is at information level (e.g., confirmation that the program is working as expected).

Debug: Debug-level messages (e.g., messages that contain information normally of use only when debugging a program). Setting the Syslog Output Level to Debug may cause very verbose output.

Emergency
Alert
Critical
Error
Warning
Notice
Info
Debug

Syslog Server:

Server Address: Enter the IP address of the syslog server.

Port Number: Enter the desired port number for syslog. The default protocol for sending syslogs is UDP with a default port of 514. The default port for TCP syslog messages is 1468. To listen on a different port for TCP messages, enter any port value from 1 to 65535.

Protocol: At the dropdown select the syslog protocol to use (*UDP* or *TCP*).

UDP
TCP

Buttons:

Cancel: Click to ignore webpage changes.

Apply: Click to save webpage settings to running-config.

Maintenance

This menu section lets you configure backup, restore, save startup-config, set factory defaults, upgrade firmware, and reboot the switch.

Maintenance > Backup

This page lets you perform a backup of a selected Configuration file. The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch. There are three system files that can be backed up: Running Config, Startup Config, and Default Config. Note that the TFTP server or SCP server must be running and configured.

Parameter descriptions:

Protocol: At the dropdown select the backup protocol to use:

https: Use secure HTTP protocol to back up the selected file (default).

http: Use HTTP protocol to back up the selected file (not secure).

scp: Secure Copy Protocol helps transfer computer files securely from a local to a remote host. The underlying Secure Shell (SSH) protocol provides authentication and security.

tftp: Trivial File Transfer Protocol is a UDP protocol used to transfer files. TFTP can read or write files from or to a remote server. TFTP does not require user authentication and is simpler to use than SCP.

ftp: Use File Transfer Protocol to back up the selected file.

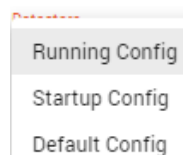


Datastore: At the dropdown select the desired file type:

Running Config: A virtual file that represents the currently active configuration on the switch. This file is volatile.

Startup Config: The startup configuration for the switch, read at boot time.

Default Config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.



Address E.g. (192.168.60.1): Enter the IP address of the remote TFTP server or remote SCP host.

File Path: Enter the name of and path to the file to be transferred (a plain text file in CLI command format).

Buttons:

Apply: Click to perform a backup of the selected file.

Maintenance > Restore

This page lets you restore a selected backed up Configuration file. The system files that can be restored are Running Config and Startup Config.

Parameter descriptions:

Protocol: At the dropdown select the backup protocol to use:

https: Use secure HTTP protocol to restore the selected file (default).

http: Use HTTP protocol to restore the selected file (not secure).

scp: Secure Copy Protocol helps transfer computer files securely from a local to a remote host. The underlying Secure Shell (SSH) protocol provides authentication and security.

tftp: Trivial File Transfer Protocol is a UDP protocol used to transfer files. TFTP can read or write files from or to a remote server. TFTP does not require user authentication and is simpler to use than SCP.

ftp: Use File Transfer Protocol to restore the selected file.

https
http
scp
tftp
ftp

Datastore: At the dropdown select the desired

Running Config: A virtual file that represents the currently active configuration on the switch. This file is volatile.

Startup Config: The startup configuration for the switch, read at boot time.

Running Config
Startup Config

Address E.g. <username><password>@192.168.60.1: Enter the IP address of the remote TFTP server or the remote SCP host.

File Path: Enter the name of and path to the file to be transferred (a plain text file in CLI command format).

Buttons:

Apply: Click to restore a selected backed up file.

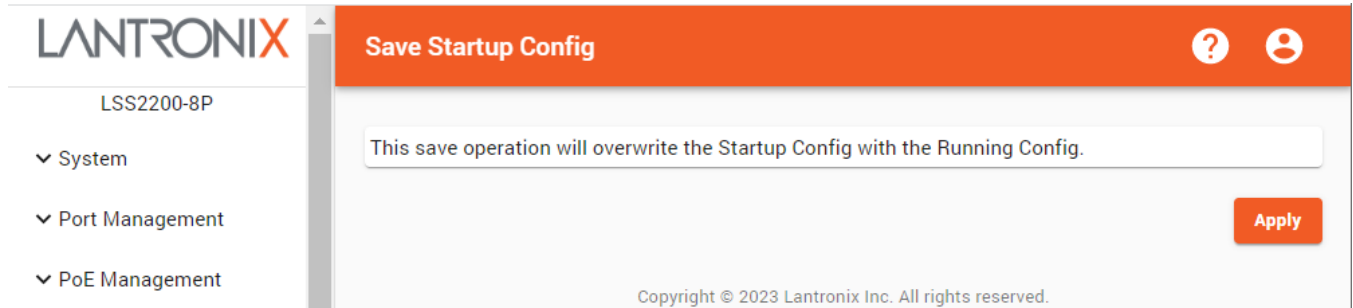
Note: Restoring a config can take a long time (typically 30 seconds or more). Do not interrupt the operation; it is important to wait for the operation to complete.

Note: Successful completion of a Running Config restore operation may cause the current Web UI session to close. For example, if the restored config changes the Time Zone, it can cause the web token to expire, thereby requiring you to log in again. Again, wait for the operation to complete before taking any action in the Web UI, including Logout.

Maintenance > Save Startup Config

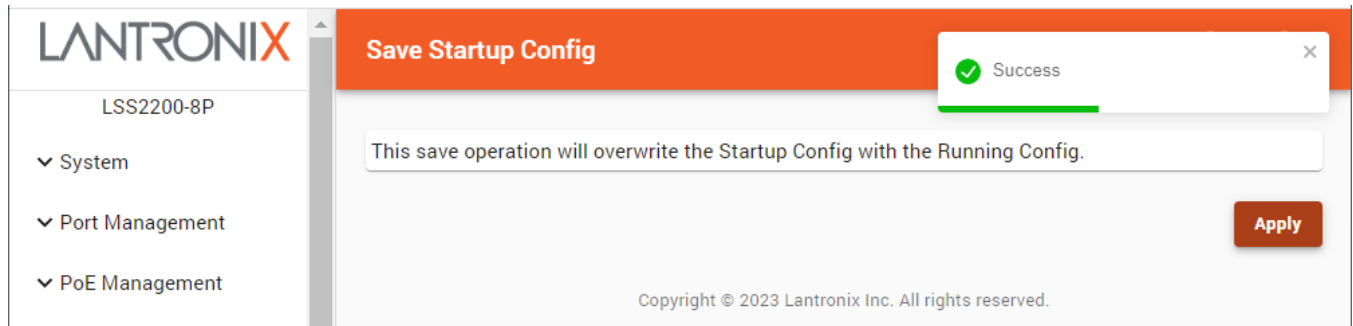
Navigate to the Maintenance > Save startup-config menu path to display the Save Startup Config page.

This page lets you copy running-config to startup-config, thereby ensuring that the currently active configuration will be used at the next reboot.



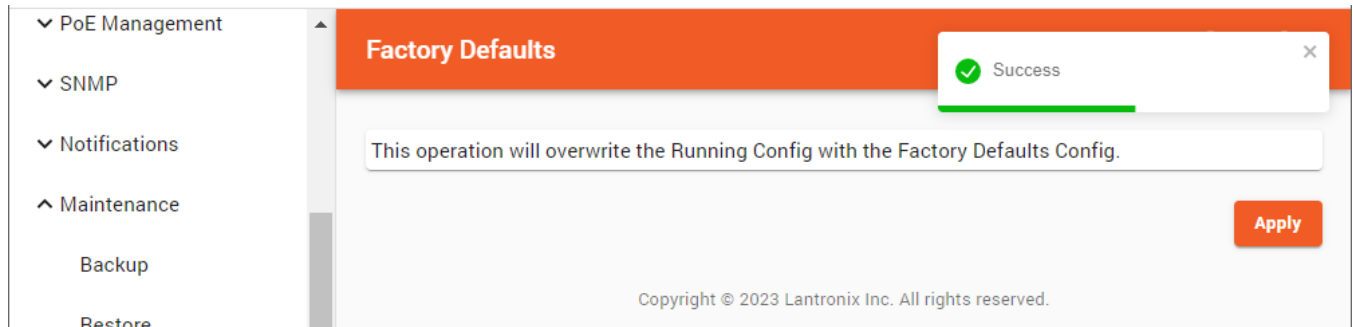
Note: This save operation will overwrite the Startup Config with the Running Config.

Click the **Apply** button to start the save process. When the save operation is done a pop-up message displays showing the result: *Success* or *Error*. The message clears automatically after about 5 seconds.



Maintenance > Factory Defaults

This operation will overwrite the Running Config with the Factory Defaults Config.



When the restore to factory defaults operation is done, a pop-up message displays showing the result: *Success* or *Error*. The message clears automatically after about 5 seconds. (There is no confirmation; the restore operation starts immediately when you click Apply.)

Buttons:

Apply: click the button to start the restore to factory defaults process

Messages:

This operation will overwrite the Running Config with the Factory Defaults Config.

Applying Changes

Maintenance > Firmware Update

This page lets you upgrade the switch firmware. You can browse to and select a file or fetch with an entered URL.

Note: After upgrading from v1.5.0.0R16 to v1.6.0.0R6, reload defaults and save or do a factory reset.

Note: Updating firmware can take a long time (typically 2 to 3 minutes), and a successful update causes the system to reboot onto the new firmware image (typically 3 to 4 more minutes). Do not interrupt the operation; it is important to wait for the operation to complete. The Web UI will continue polling and will present the Login page once the reboot is complete.

Parameter descriptions:

File Upload: Click Browse and select the desired firmware file to upload.

Or fetch with URL:

Protocol: At the dropdown select the protocol to use for the firmware update:

https: Use secure HTTP protocol to restore the selected file (default).

http: Use HTTP protocol to restore the selected file (not secure).

scp: Secure Copy Protocol helps transfer computer files securely from a local to a remote host. The underlying Secure Shell (SSH) protocol provides authentication and security.

tftp: Trivial File Transfer Protocol is a UDP protocol used to transfer files. TFTP can read or write files from or to a remote server. TFTP does not require user authentication and is simpler to use than SCP.

ftp: Use File Transfer Protocol to restore the selected file.

Address E.g. 192.168.60.1: Enter the IP address of the selected file server.

File Path: Enter the path to the selected file.

Buttons:

Apply: Click to perform the firmware update with the selected parameters.

https
http
scp
tftp
ftp

Maintenance > Reboot

This page lets you reboot the switch immediately, after a set time period, or on a defined schedule. Any config files or scripts that you saved in the switch will be available afterwards.

Parameter descriptions:

Reboot Schedule:

Date: Enter or select the date for the reboot in the format *mm/dd/yyyy*. You can also select *Clear* or *Today* from the calendar.

Time: Enter or select the time for the reboot in the format *hh:mm* and *AM* or *PM*.

Click the **Apply** button and verify the “*Are you sure ...?*” prompt to save the reboot schedule changes.

Reboot Delay:

Remaining time until reboot (HH:MM:SS): Displays the amount of time left before the reboot in hours, minutes and seconds.

Delay (HH:MM:SS): Enter the amount of time you want the switch to wait before the reboot, in hours, minutes and seconds.

Click the **Apply** button to save the reboot delay parameters.

Reboot Now:

Verify the “*Are you sure you want to reboot the device?*” prompt and click the **Reboot** button to start the reboot process immediately.

Buttons:

Cancel: Click to ignore webpage changes.

Clear Pending Reboot: Click to clear an upcoming reboot schedule or delayed reboot. The Success message displays, but the newly created Reboot schedule time still exists. It will continue to exist until you refresh the web browser.

ConsoleFlow

This page lets you configure ConsoleFlow™ parameters. This page has four sections: the Status, Configuration, ConsoleFlow Connection 1, and Connection 2 sections as shown and described below.

ConsoleFlow is Lantronix Cloud-hosted or On premise management platform that provides a single pane of glass for centralized management and automated monitoring of deployed Lantronix devices, along with real-time notifications, managed APIs and data dashboards. **Note:** A ConsoleFlow subscription is required for access to ConsoleFlow features. For more information see <https://www.lantronix.com/consoleflow/>.

The ConsoleFlow page has four sections (Status, Configuration, Connection 1, and Connection 2) as shown and described below.

Status section:

The screenshot shows the Lantronix ConsoleFlow interface. The top navigation bar is orange with the Lantronix logo on the left, the text 'ConsoleFlow' in the center, and a help icon and user profile icon on the right. Below the navigation bar, the device identifier 'LSS2200-8P' is displayed. The left sidebar contains a list of navigation items: System, Port Management, PoE Management, SNMP, Notifications, Maintenance, ConsoleFlow (selected), and Lantronix Provision Manager. The main content area is titled 'Status' and displays the following information:

- Client State:** Exited
- Device ID:** 00204AAT7IC0VD10F3DWTTXJMV2ET51A
- Device Key:** <Configured>
- Last Status Update:** <Not Available>
- Last Content Check:** <Not Available>
- Available Firmware Updates:** <Not Available>
- Available Configuration Updates:** <Not Available>

Parameter descriptions:

Client State: Displays the current state of the ConsoleFlow client (e.g., *Started*, *Connected*, *Running*, *Exited*, *Invalid credentials* or *<Not Yet Started>*).

Device ID: Displays the assigned 32-character device ID for the switch. The Device ID may be provisioned through Lantronix Provision Manager. **Note:** Device ID can only be provisioned once. It will persist across resets.

Device Key: Shows whether the switch Device Key has been configured. (e.g., *<Configured>*). **Note:** Device Key may be configured via the Lantronix Provision Manager (LPM).

Last Status Update: Shows how long since the last status update from the device to ConsoleFlow.

Last Content Check: Shows how long since the content (firmware/configuration) was checked by the device.

Available Firmware Updates: If automatic firmware update is disabled, this is a list of updates available on ConsoleFlow.

Available Configuration Updates: If automatic configuration update is disabled, this is a list of updates available on ConsoleFlow.

ConsoleFlow Configuration section:

Configuration		
Device State	Device Name	Device Description
Enabled	LSS2200-8P-T51A	Lantronix LSS2200-8P
Status Update Interval	Content Check Interval	Apply Firmware Updates
1	24	Enabled
Apply Configuration Updates	Remote Access Local Port	Active Connection
Always	0	Connection 1

Parameter descriptions:

Device State: At the dropdown select *Enabled* or *Disabled* for ConsoleFlow operation on this switch.

Device Name: Enter the desired name for this switch. The default is *LSS2200-8P*.

Device Description: Enter a name for this switch. The default is *Lantronix LSS2200-8P Device*

Status Update Interval: Select the amount of time in minutes between updates (1-1440 minutes).

Content Check Interval: Select the amount of time in minutes between content checks (1-2160 minutes).

Apply Firmware Updates: At the dropdown select *Enabled* to automatically apply available firmware upgrades to the switch. Otherwise select *Disabled*.

Apply Configuration Updates: At the dropdown select when config updates (changes) should be applied:

Never: Do not apply config updates ever.

If unchanged: Apply config updates only if no changes have been made locally.

Always: Apply config updates whenever available.



Remote Access Local Port: Select the desired local port for remote access (the local port for ConsoleFlow connections). When configured, a total of 16 consecutive ports will be reserved.

Active Connection: At the dropdown select *Connection 1* or *Connection 2* as the activated connection. The default is *Connection 1*.

Message: 400 Error: Invalid modify request – LOCAL_PORT is not 0 or in the range 1024..65504

ConsoleFlow Connection 1 and Connection 2 sections:

The screenshot shows the Lantronix ConsoleFlow configuration page. The left sidebar contains a navigation menu with options: System, Port Management, PoE Management, SNMP, Notifications, Maintenance, ConsoleFlow (selected), and Lantronix Provision Manager. The main content area is titled 'ConsoleFlow' and contains two connection configuration sections, 'Connection 1' and 'Connection 2'. Each section has a grid of settings:

- Host:** api.consoleflow.com
- Connects to:** Cloud (for Connection 1) / On-Premise (for Connection 2)
- Port:** 443
- Secure Port:** Enabled
- Validate Certificates:** Enabled
- Local Port:** 0
- MQTT Security:** Enabled
- MQTT Local Port:** 0
- Use Proxy:** False
- Proxy Type:** SOCKS5
- Proxy Host:** (empty)
- Proxy Port:** 80
- Proxy Username:** (empty)
- Proxy Password:** (empty)

At the bottom right of the configuration area are 'Cancel' and 'Apply' buttons. A copyright notice at the bottom center reads: 'Copyright © 2022 Lantronix Inc. All rights reserved.'

Parameter descriptions:

Host: Enter the host name or IP address for this connection (Connection 1 top, Connection 2 bottom) (e.g., *api.consoleflow.com*).

Connects to: At the dropdown, select the ConsoleFlow connection type to use for Connection 1 / Connection 2:

Cloud: Use the Cloud-based version of ConsoleFlow for Connection 1 / Connection 2 (default).

On premise: Use the on-premise version of ConsoleFlow for Connection 1 / Connection 2.

Port: Select the port number for this connection (Connection 1 or 2). The default is port 443. Port 443 is used explicitly for HTTPS services and it is the standard port for HTTPS (encrypted) traffic.

Port: Select the desired port number. The default is port 443.

Secure Port: At the dropdown select port security for this port (*Enabled* or *Disabled*). The default is *Enabled*.

Validate Certificates: At the dropdown select *Enabled* to have SSL certificates validated by the switch. Otherwise select *Disabled*. The default is *Enabled*.

Local Port: Select the desired local port number. The default is 0.

MQTT Security: At the dropdown select *Enabled* to enable MQTT security. Otherwise select *Disabled*. The default is *Enabled*. MQTT (originally “MQ Telemetry Transport”) is a Client Server publish/subscribe messaging transport protocol.

MQTT Local Port: Displays the local port to be used for MQTT. The default is local port 0.

Use Proxy: Displays whether a Proxy is used (*True* or *False*). The default is *False*.

Proxy Type: Displays the type of Proxy Server being used (*SOCKS5*). Valid selection:

SOCKS5 : The SOCKS Internet protocol exchanges network packets between a client and server through a proxy server. SOCKS5 optionally provides authentication so only authorized users may access a server. A SOCKS server proxies TCP connections to an arbitrary IP address, and provides a means for UDP packets to be forwarded. For SOCKSv5 see [RFC 1928 - SOCKS Protocol Version 5 \(ietf.org\)](https://www.ietf.org/rfc/rfc1928.txt). SOCKS5 is currently the only option for the LSS2200-8P Proxy Type.

Proxy Host: Displays the IP address or host name of the Proxy server.

Proxy Port: Displays the port number of the Proxy server to be used. The default is port 80.

Proxy Username: Displays the user name for the proxy for this connection.

Proxy Password: Displays the password for the proxy for this connection.

Buttons:

Cancel: Click to ignore the webpage changes.

Apply: Click to apply the webpage changes.

Managed Devices Auto-Discovery

The LSS2200-8P can use ConsoleFlow to discover the devices connected to the switch interfaces (ports) as follows:

- For LLDP devices: MAC Addr, Description, Name, and Model.
- For non-LLDP devices: base telemetry query.

Note that low-power PDs typically do not support LLDP. So in many cases, ConsoleFlow can report just PD Class, which indicates if a PD is connected to that local port.

Lantronix Provisioning Manager (LPM)

Lantronix Provisioning Manager (LPM) allows easy administration of Lantronix Remote Environment Management (REM) devices, IoT gateways and device servers. With LPM, administrators can quickly update firmware, update configuration, and provision one or more devices at the same time as well as recover devices via serial.

The LPM application provisions, configures, and updates Lantronix Console Managers and IoT Gateways for local site installations and deployments. LPM can handle changes to a single Lantronix device or support updating a group of them concurrently. As a self-contained utility, LPM does not have any dependencies on the target OS environment, making it easy to use without needing any external Internet access. LPM is available for Windows, Linux and Mac OS.

For your existing deployments, LPM can scan for and provision Lantronix managed Ethernet switches dynamically to integrate with Lantronix ConsoleFlow.

The screenshot shows the Lantronix Provision Manager web interface. The top navigation bar includes the Lantronix logo and the title 'Lantronix Provision Manager'. The left sidebar lists various management categories: System, Port Management, PoE Management, SNMP, Notifications, Maintenance, ConsoleFlow, and Lantronix Provision Manager. The main content area displays the following configuration and status information:

- Admin State:** Enabled
- Status:**
 - Client State: Running
 - Valid Queries: 0
 - Unknown Queries: 0
 - Erroneous Packets: 0
 - Errors: -
 - Last Connection: 0.0.0.0/0

At the bottom right, there are 'Cancel' and 'Apply' buttons. A copyright notice at the bottom reads: Copyright © 2023 Lantronix Inc. All rights reserved.

Parameter descriptions:

Configuration:

Admin State : At the dropdown select *Enabled* or *Disabled* as the LPM admin state. The default is LPM *Enabled*.

Status :

Client State : Displays the current status of the LPM client (e.g., *Running*).

Valid Queries : Displays the current number of LPM valid queries.

Unknown Queries : Displays the current number of LPM unknown queries.

Erroneous Packets : Displays the current number of LPM errored packets recorded.

Errors : Displays the current number of LPM errors recorded.

Last Connection : Displays the IP address of the last successful connection in the format 0.0.0.0/0.

Buttons:

Cancel: Click to cancel webpage settings.

Apply: Click to save webpage settings to running-config.

Supported Features

Lantronix Provisioning Manager (LPM) supported features are based on the capabilities of the device. See the LPM webpage at <https://docs.lantronix.com/products/lpm/5.x/>. View the Lantronix Provisioning Manager User Guide at <https://docs.lantronix.com/products/lpm/latest/>

Discovering Devices

LPM automatically discovers devices of the type(s) selected at the device type selection screen. It discovers devices only on the same subnet as the computer running LPM or in the IP range configured in Network Settings. LPM discovers devices by network interface. If a device has two network interfaces connected, LPM will list it twice. For more information see the LPM webpage at <https://docs.lantronix.com/products/lpm/5.x/discovery/>.

4. Troubleshooting

See the LSS2200-8P install Guide for detailed troubleshooting information.

5. Regulatory Agency Information

See the LSS2200-8P install Guide for all regulatory agency compliance information.

6. MobileApp

See the LSS2200-8P MobileApp User Guide for Mobile App information.

**Lantronix Corporate Headquarters**

48 Discovery, Suite 250
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support

Online: <https://www.lantronix.com/technical-support/>

Sales Offices

For a current list of our domestic and international sales offices, go to the Lantronix web site at www.lantronix.com/about/contact.